

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR
FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



**“PROYECTO DE MIGRACION DEL PROTOCOLO IPV4 AL IPV6
UTILIZANDO EL MECANISMO DE DOBLE PILA (DUAL STACK) EN
LA EMPRESA BP SUPPORT”**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

CRUZ OJEDA, JOSE RAUL

Villa El Salvador

2018

DEDICATORIA

Detrás de este proyecto se agradece a todas las personas que me dieron su apoyo y siempre han creído en mí.

Dedico este trabajo primero a Dios, por haberme dado salud, fuerza en los momentos complicados y vida para poder culminar el proceso académico en la universidad.

A mis padres: Víctor Raúl Cruz Neyra, a ese gran padre que es, quien ha sido parte fundamental en mi preparación académica y darme ánimos en los días malos y buenos, gracias papá; a Socorro Ojeda García mi madre, quien siempre me apoya hasta en lo más mínimo, en mi quehacer diario, por su preocupación constante y haberme brindado sus conocimientos desde que era pequeño, Gracias mamá.

A mi hermano Jeyner Cruz Ojeda, por haber estado siempre conmigo, más que mi hermano es mi confidente ese gran amigo al cual nunca me gustaría perder, ahora el sigue su carrera y sé que le va a ir muy bien. Gracias Jeyner.

A Don Luchito un buen amigo de la familia, que no se encuentra de manera física con nosotros, por ese apoyo que me dio durante muchos años y ahora se le extraña bastante, sé que estés donde estés me apoyas y a toda nuestra familia. Gracias Luchito.

AGRADECIMIENTO

Agradezco primero a Dios, a mis padres por haberme dado la vida y siempre me han dado su apoyo en las buenas y también en las malas a pesar de errores que cometí en algunos años, ellos han sido parte fundamental en este proceso académico y personal, y por último a mi asesor de tesina el Ing. Julio Quispe, quien me tuvo mucha paciencia y ayudó con sus conocimientos para poder culminar este proyecto.

INDICE

INTRODUCCIÓN	1
CAPITULO I: PLANTEAMIENTO DEL PROBLEMA	3
1.1. Descripción de la realidad problemática	3
1.2. Justificación del Proyecto	5
1.3. Delimitación del Proyecto	7
1.3.1. Teórica	7
1.3.2. Temporal	7
1.3.3. Espacial	7
1.4. Formulación del Problema	7
1.4.1. Problema General	7
1.4.2. Problemas Específicos	7
1.5. Objetivos	8
1.5.1. Objetivo General	8
1.5.2. Objetivos Específicos	8
CAPITULO II: MARCO TEORICO	9
2.1 Antecedentes de la Investigación	9
2.1.1 Antecedentes Internacionales	9
2.1.2 Antecedentes Nacionales	19
2.2 Bases teóricas	23
2.2.1 Modelo OSI	23
2.2.2 Redes de Computadoras	24
2.2.3 Medios de transmisión	24
2.2.4 Direccionamiento IP	25
2.2.5 Protocolos de comunicaciones	26
2.2.6 Protocolo de internet	27
2.2.7 IPv4	27
2.2.8 IPv6	29
2.2.9 Comparación entre los protocolos IPv4 e IPv6	34
2.2.9.1 Dirección	34
2.2.9.2 Asignación de direcciones	35
2.2.9.3 Máscara de dirección	35
2.2.9.4 Prefijo de la dirección	35
2.2.9.5 ARP	36
2.2.9.6 Configuración	36

2.2.9.7	Fragmentos.....	36
2.2.9.8	Cabecera IP	37
2.2.9.9	Direcciones privadas y públicas	37
2.2.9.10	Cambio de numeración	38
2.2.10	Beneficios de la transición de IPv4 a IPv6	39
2.2.11	Mecanismos de transición	40
2.3	Definición de términos básicos.....	44
CAPITULO III: DESARROLLO DEL OBJETIVO DE SUFICIENCIA		47
3.1	Situación actual de BP SUPPORT	47
3.2	Modelo de transición del protocolo IPv4 a IPv6.....	50
3.2.1	Fase de planeación de IPv6	50
3.2.2	Fase de implementación del protocolo IPv6	51
3.2.3	Fase de pruebas de funcionalidad de IPv6.....	52
3.3	Cronograma de Actividades	53
3.4	Aplicando Dual Stack.....	54
3.5	Aplicando Túneles.....	58
3.6	Acerca de Traducción	61
3.7	Analizando los métodos	61
3.8	Costos de implementación	63
CONCLUSIONES		66
RECOMENDACIONES		67
BIBLIOGRAFIA.....		68
ANEXOS.....		71

LISTADO DE FIGURAS

Figura 1: Modelo OSI	23
Figura 2: Datagrama IPv4	27
Figura 3: Datagrama IPv6	29
Figura 4: Formato dirección Unicast.....	32
Figura 5: Dirección Multicast	32
Figura 6: Tunnelización IPv6 a IPv4.....	41
Figura 7: Método Dual Stack.....	42
Figura 8: Método de Traducción.....	43
Figura 9: Diagrama de Gantt.....	53
Figura 10: Topología A Utilizar Con Doble Pila	54
Figura 11: Prueba De Ping Desde PC0 Hacia El Servidor Usando Ipv4.....	56
Figura 12: Prueba De Ping Desde PC1 Hacia El Servidor Usando Ipv6.....	57
Figura 13: Topología a utilizar con tunnelización 6over4	58
Figura 14: Prueba de ping desde PC0 hacia el servidor usando IPv6	60

LISTADO DE TABLAS

Tabla 1: Principales ISP con Ipv6 en el Perú	20
Tabla 2: Miembros del NAP Perú	21
Tabla 3: Direccionamiento de clientes y servidores	49
Tabla 4: Cuadro comparativo de los métodos de migración	62
Tabla 5: Software que soporta IPv6	63
Tabla 6: Hardware que soporta IPv6	64
Tabla 7: Costos de capacitaciones	64
Tabla 8: Presupuesto final	65

INTRODUCCIÓN

El creciente interés de internet en los últimos años ha sido motivado por el desarrollo que han adquirido las computadoras y las redes que ellas lo conforman. La evolución de los dispositivos que han podido acceder como teléfonos inteligentes, tablets, relojes inteligentes, televisores entre otros han limitado las direcciones IP, esto en razón a la demanda de los servicios que se generan a través de él. Previendo las limitaciones que a futuro existirían con la capacidad de direccionamiento se desarrolló un protocolo IP llamado IPv6, el cual posee muchas mejoras y la característica más sobresaliente es que nos ofrece una mayor capacidad de direcciones IP con respecto a su antecesor Ipv4.

Las tecnologías que son dependientes del protocolo de direccionamiento IP han evolucionado con el pasar del tiempo, dando origen a nuevos campos de acción como empresariales y educativos entre otros, los cuales requieren del protocolo IPv6 para la mayor utilización de la calidad y las aplicaciones que están emergiendo de la evolución de la tecnología. Dando respuesta a esta evolución y teniendo como herramienta de optimización y mejora el protocolo de internet IPv6, este direccionamiento se ha venido implementando con la premisa de dar solución a otro tipo de encaminamiento pero sin afectar los procesos y las aplicaciones que están trabajando sobre el protocolo de internet IPv4; en general lo que se pretende es hacer una migración a IPv6 conviviendo en paralelo con el protocolo anterior para no impactar desfavorablemente la red donde se esté aplicando este proceso.

Teniendo este planteamiento se quiere implementar una transición de IPv4 a IPv6 utilizando el método Dual Stack permitiendo que los dos protocolos operen

sin denegar los servicios que cada uno ofrece, entregando un planteamiento a la solución de la transición.

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

La creación de las redes de computadoras para interconectar dispositivos creadas en finales de los años 50's han evolucionado en las últimas 4 décadas. Los desarrolladores de las distintas redes tenían formas de comunicación distintas; por esto crearon un conjunto de protocolos con el ánimo de estandarizar las conexiones para todos los fabricantes. (Iñigo, 2009)

Después de una estandarización de los protocolos de comunicación entre desarrolladores, se creó un protocolo el cual puede identificar todos los dispositivos conectados a la red mediante direcciones IP, por medio de etiquetas conformadas por 4 octetos de bits, las cuales entregan un poco menos de 4300 millones de direcciones (L.M, 2012).

Con la evolución de los dispositivos electrónicos que se pueden conectar a la internet, y el apogeo en el mundo de los nuevos productos y servicios a los cuales los usuarios podían acceder a la red (Iñigo, 2009), el sistema binario de 32 bits se empezó a ver limitado para otorgar direcciones de acceso a internet.

Analizando esta preocupante proyección se desarrolló un protocolo de direccionamiento más amplio, basándose en un sistema hexadecimal que contiene 8 grupos de 16 bits (128 bits); como es un número bastante grande, una comparación pertinente a la cantidad de direcciones es que puede ser igual a la cantidad de granos de arena que existen en la tierra (6sos.org, 2004).

Teniendo en cuenta esta proyección tan poco alentadora, LACNIC (Latin American Caribbean Network Information Centre) el cual es el ente que distribuye y asigna las direcciones IP, ha creado un proceso para el agotamiento de las direcciones IPv4. Este aparte tiene como objeto dar a conocer los procesos y etapas que involucran el agotamiento gradual de las direcciones IPv4, dependiendo de unas buenas políticas de administración para las que aún quedan en la red (LACNIC, Fases de Agotamiento de IPv4., 2016).

La realidad de esta preocupante proyección que entrega LACNIC evita el crecimiento de internet, detiene el crecimiento del país, restringe las conexiones a la red, incrementa los costos de mantenimiento de las interconexiones, limitan los servicios que internet puede desplegar e impedir la implantación de tecnologías emergentes de nueva generación y por consiguiente el retraso tecnológico en comparación al resto del mundo (MINTIC., 2011).

Además hay que tener en cuenta que cuando el protocolo IPv6 sea mandatorio, se generarán más gastos en la implementación por la demanda de la mayoría de usuarios que optaran por la migración hasta que sea obligatorio (Mexico, s.f.).

Según un informe hecho en la Escuela de Ingeniería Eléctrica y Electrónica de la Universidad del Valle "Diseño e implementación de una red de IPv6 para

transición eficiente desde IPv4" los costos que son necesarios asumir para la adquisición de equipos donde se tienen que aplicar mecanismos de transición, hace que las entidades piensen en acoger IPv6 hasta que se difunda totalmente en todo el país. Cabe aclarar que los protocolos descritos no son compatibles y por un tiempo tendrán que convivir en las redes de telecomunicaciones, por medio de métodos que ayuden a trabajar paralelamente con los dos protocolos, mientras que se puede adoptar completamente en las redes IPV6.

Todas estas falencias y dudas en la adopción de IPv6 contextualizan el motivo de la investigación que se desea hacer, específicamente en realizar una migración con el más mínimo impacto a la red.

1.2. Justificación del Proyecto

A inicios del año 2011 la IANA (Internet Assigned Numbers Authority) entregó el último grupo de direcciones IPv4 que quedaba disponible (33 millones) a la APNIC que es la entidad encargada de distribuir las direcciones IP en Asia. De acuerdo con esto Latinoamérica ya está usando sus reservas de direcciones IPv4, lo que conlleva a la inminente transición al protocolo IPv6.

IPv4 ha sido hasta el momento el protocolo más usado en internet, pero entró en una fase de agotamiento irreversible. Por esta razón, quiero impulsar la migración hacia el protocolo IPv6, esto con el fin de alentar a los operadores locales a acelerar la transición en beneficio de los usuarios finales.

La migración a una nueva tecnología produce inseguridad al no tener la certeza si tendrá impactos negativos en la red con respecto al estado anterior del traslado. Las razones son el desconocimiento del protocolo IPv6, asumiendo que el tema de adaptación de la red es muy especializado, falta de personal

certificado para dictar conferencias y charlas, que multipliquen la información acerca del tema y puedan implementar la migración en los diversos campos de las organizaciones del país y por último el costo de la adquisición de los equipos necesarios para la implementación (Calderón, 2012).

Esta investigación ayudará a clarificar dudas a nivel de implementación de la migración de IPv4 a IPv6, sirviendo como punto de apoyo para que las personas o entes interesados en la adopción de IPv6 conozcan las características de desempeño del protocolo IPv6 cuando es ejecutado en la red.

En la actualidad hay muchos servicios que se desarrollan en el protocolo IPv4, por esto hay que tener un estado de convivencia entre los dos protocolos de enrutamiento por algún periodo de tiempo. Debido a que estos protocolos tienen que trabajar en paralelo para poder tener los dos servicios (IPv4-IPv6) se trabajará el despliegue con un sistema tipo Dual Stack (doble pila).

Teniendo en cuenta que la adopción de nuevas tecnologías es sinónimo de desarrollo para cualquier sociedad que quiera estar vigente en el mundo moderno, es importante dar un soporte investigativo que promueva reflexiones comparativas para dar un salto en el camino de la evolución o por lo menos ir a la par con el mundo moderno.

1.3. Delimitación del Proyecto

1.3.1. Teórica

En el siguiente trabajo abarca sobre la migración de protocolos usando doble pila (dual stack), el cual presenta una serie de pasos para una correcta transición hacia IPv6.

1.3.2. Temporal

La propuesta de migración del protocolo IPv4 al IPv6 se desarrollará en 3 meses, comenzando en julio del 2019 y terminando en setiembre del 2019.

1.3.3. Espacial

El proyecto se desarrollará en la empresa BP SUPPORT SOCIEDAD ANONIMA CERRADA, ubicada en la Avenida Javier Prado Oeste 757, Magdalena del Mar.

1.4. Formulación del Problema

1.4.1. Problema General

¿Cómo realizar la migración del protocolo (IPv4) al protocolo (IPv6)?

1.4.2. Problemas Específicos

¿Cómo está la situación actual de la red interna en la empresa BP SUPPORT?

¿Cómo asegurar que métodos de migración se pueden utilizar en la actualidad?

¿Cómo asegurar una correcta migración?

1.5. Objetivos

1.5.1. Objetivo General

- Elaborar el proyecto de migración del protocolo IPv4 al IPv6 en la empresa BP SUPPORT

1.5.2. Objetivos Específicos

- Recopilar información de la situación actual de la red interna en la empresa BP SUPPORT.
- Analizar los diferentes métodos de migración vigentes sobre IPv6, mediante un cuadro comparativo.
- Diseñar el proyecto de migración y realizar las pruebas.

CAPITULO II: MARCO TEORICO

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes Internacionales

Respecto a tesis, proyectos o trabajos de investigación relacionados al tema se encontraron los siguientes:

Estados Unidos

Para Estados Unidos, según (Baltazar, 2017) en su tesis titulada **MODELO DE REFERENCIA DE TRANSICION DE IPv4 A IPv6 PARA EL SECTOR GOBIERNO DE PERU**, nos menciona como este país ha ido adaptándose a este cambio para la implementación a IPv6.

En agosto de 2005, la "Office of Management and Budget – OMB", de los Estados Unidos - EEUU, emitió el Memorando M-05-22, con el asunto "Transition Planning for Internet Protocol Version 6 (IPv6)" (Budget., 2005). En este documento se establece un conjunto de acciones que deben realizar cada una de las agencias de gobierno de los EEUU para el despliegue de IPv6 entre los años 2006 - 2008. De manera resumida, se menciona alguna de estas acciones

previstas hacer realizadas (2006 – 2008) por cada una de las agencias de gobierno de los EEUU:

Asignación de un responsable para realizar las coordinaciones pertinentes,

- Realizar el inventario del equipamiento informático y de comunicaciones para determinar la compatibilidad con el nuevo protocolo IPv6.
- Análisis de impacto y riesgos para la transición a IPv6.
- Plan de transición IPv6.
- Asegurar en las nuevas adquisiciones de TI (Tecnologías de Información) el soporte de ambos protocolos (IPv4 – IPv6), entre otros (Budget., 2005).

En el citado memorando, también, se designa a la “National Institute for Standards and Technology – NIST”, de ser necesario, para el desarrollo de las normas y ensayos para la implementación del IPv6 en el gobierno federal de EEUU y designa también a la “Federal Acquisition Regulation - FAR”, de ser necesario, para el desarrollo de una modificación para el uso por todas las agencias de gobierno (Budget., 2005).

En el 2008, el NIST, publica el documento “A profile for IPv6 in the U.S. Government – Version 1.0”, en el cual se recomienda una lista de RFCs y consideraciones técnicas mínimas de seguridad, calidad de servicio, multicast, gestión de red y movilidad para la adquisición de equipamiento (Hosts, routers y dispositivos de seguridad) con IPv6 en las agencias de gobierno (Technology. N. I., 2008).

En el 2009, el NIST, publica el documento “USGv6 Test Methods: General Description and Validation”, en la cual se establece un programa de pruebas mínimos de IPv6 hacer realizados por laboratorios acreditados con la ISO/IEC 17025 (Technology. N. I., USGv6: Test Methods:General Description and

Validation. , 2009). Estados Unidos, a través de la NIST, actualiza continuamente el programa de pruebas para el protocolo IPv6, para lo cual ha firmado memorandos de entendimiento con el programa de prueba “IPv6 Ready Logo”, para el uso de sus especificaciones de prueba como base inicial para el programa de pruebas del NIST en relación a IPv6 (Technology. N. I., USGv6: Test Methods:General Description and Validation. , 2009). Asimismo, considera el uso de los parámetros de pruebas establecido por el Department of Defense - DoD en su programa “The DoD IPv6 Standards Profile for IPv6 Capable Products”.

En Mayo del 2009, la agencia federal Chief Information Officers – CIO, en base a las buenas prácticas Público/Privadas, publica el documento denominado “Planning Guide/Roadmap Toward IPv6 Adoption within the US Government Version 1.0” (Architecture and Infrastructure Committee, Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government” (the “Roadmap”), Version 1.0., 2009), y en Julio del 2012, la misma agencia (CIO), publica la versión 2.0 (Architecture and Infrastructure Committee, Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government”, Version 2.0., 2012). En estos documentos se evidencia que las agencias de gobierno, a través de sus oficinas de tecnología, cuentan con una arquitectura empresarial madura (Arquitectura de negocio, Arquitectura de Aplicaciones y Arquitectura Tecnológica), que es soportada por una infraestructura tecnológica que permite la integración, interoperabilidad, seguridad, etc., de los servicios de red entre las agencias de gobierno, con un fin compartido, la de tener un framework que soporte todos sus servicios de TI de forma estándar, orientándose a llegar a ser un gobierno electrónico. La agencia federal CIO, realiza un análisis del estado

actual tecnológico y normativo, para determinar la línea base que les permita establecer las estrategias de transición a una arquitectura empresarial soportada por IPv6, para lo cual, considera tres etapas importantes, basada en la RFC 5211:

- Etapa de preparación,
- Etapa de transición y
- Etapa post-transición.

En ese sentido, Estado Unidos, al tener diversas metodologías maduras de gestión de sus servicios de TI, considera un plan que le permita desplegar IPv6 en cada una de estas metodologías propias para las agencias de gobierno de ese país.

De manera general, se describe los aspectos considerados, para la etapa de preparación, el cual consiste en la elaboración del plan estratégico para realizar la transición hacia IPv6, por parte de las agencias de gobierno (Architecture and Infrastructure Committee, Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government” (the “Roadmap”), Version 1.0., 2009) (Architecture and Infrastructure Committee, Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government”, Version 2.0., 2012):

- Identificación de las prioridades de transición.
- Identificación de las actividades de transición.
- Los hitos de transición.
- Criterios de transición para las capacidades heredadas, actualizadas y nuevas.
- Dependencias.
- Riesgos y estrategias de mitigación.

- Mantenimiento de la interoperabilidad y seguridad durante la transición.
- El uso del USGv6 para expresar requerimientos específicos de las capacidades soportadas de IPv6 en la compra de productos específicos (Technology. N. I., USGv6: A Technical Infrastructure to Assist IPv6 Adoption., 2015).
- Gobierno de la transición:
 - ✓ Políticas.
 - ✓ Roles y responsabilidades.
 - ✓ Estructura de Gestión.
 - ✓ Medición del desempeño.
 - ✓ Reportes.
 - ✓ Acciones de gestión.
- Entrenamiento.
- Pruebas.

Sumado a estos aspectos, las agencias de gobierno, tienen que elaborar y presentar casos de negocio para la inversión de IPv6 basado en su estrategia de implementación y enfocado en su arquitectura empresarial establecida.

En la etapa de transición, la agencia CIO, define las siguientes acciones a realizar por parte de las agencias de gobierno:

- ✓ Acelerar del despliegue de IPv6 por parte de las agencias de gobierno.
- ✓ Creación de una agencia centralizada de autoridad de direccionamiento.
- ✓ Establecer el servicio de nombre de dominio para IPv6 (AAAA).
- ✓ Establecer los métodos de asignación de direccionamiento IP.
- ✓ Gestión de toda la red.

- ✓ Seguridad de IPv6.

Asimismo, consideran tener en cuenta los siguientes potenciales impactos en la red de las organizaciones:

- ✓ IPv6 routing
- ✓ IPv6 addressing
- ✓ IPv6 multi-homing/business continuity
- ✓ IPv6 security (firewall/IDS)
- ✓ Telework/remote access
- ✓ IPv6 device management
- ✓ IPv6 address and network management
- ✓ IPv6 SLAs
- ✓ DNS support

Por lo comentado, EEUU, expone una transición madura de IPv6 en sus agencias de gobierno, proporcionando guías metodológicas, técnicas y de pruebas, laboratorios de evaluación de equipamiento, normativa y el monitoreo del despliegue de este protocolo en las redes de sus agencias de gobierno. Para el monitoreo, la NIST, a través de la División denominada “Advanced Network Technologies Division”, crea el portal de reportes estadísticos del despliegue de IPv6 en las agencias de gobierno. Estas estadísticas, se forman considerando tres aspectos: publicación de DNS, servicio de correo electrónico y servicios Web de las agencias de gobierno. A diciembre de 2015, a través de su portal Web de monitoreo, indica que 449 agencias de gobierno publican servicios Web con IPv6, 140 tienen sus servicios de correo con IPv6 y 251 DNS han sido publicados con IPv6. Sin embargo, todavía queda una brecha de 853(Web), 483(mail) y 587

(DNS) agencias (Technology. N. I., Estimating USG IPv6 & DNSSEC External Service Deployment Status., 2016).

En el ámbito académico, EEUU, a través de la Internet2, que es la red académica y de Investigación de EEUU, participa activamente en el desarrollo y difusión de IPv6. Internet2 está conformado por comunidades de investigación y educación, el gobierno y el sector privado y se comunica a través de IPv6 con otras redes avanzadas a nivel mundial (Internet2., 2015).

España

También en España se lleva a cabo la planificación hacia IPv6, según (Baltazar, 2017) en su tesis titulada MODELO DE REFERENCIA DE TRANSICION DE IPv4 A IPv6 PARA EL SECTOR GOBIERNO DE PERU, nos menciona como España ha ido adaptándose a este cambio para la implementación a IPv6

En Abril del 2011, el Consejo de Ministros de España, aprueba el documento denominado “Plan de Fomento para la Incorporación de Protocolo de Internet IPv6 en España”, el cual tiene como objetivo dinamizar la incorporación del protocolo IPv6 (Presidencia, 2011).

Dicho Plan, a nivel general es impulsado por el Ministerio de Industria, Energía y Turismo - MITYC, y a nivel de la instituciones públicas de España, por el Ministerio de Política Territorial y Administración Pública - MPTYAP (Presidencia, 2011).

Este Plan considera inicialmente 10 medidas, las cuales están orientadas a la incorporación de IPv6 en los servicios de Internet, iniciando por el MITYC, el portal www.ipv6.es, www.060.es (administracion.gob.es) y en otros 10 portales de instituciones públicas, así como también las siguientes acciones:

- ✓ La difusión y capacitación del nuevo protocolo a las instituciones públicas, fomentando la participación público-privada;
- ✓ Apoyo en proyectos de implementación de IPv6 en el sector privado;
- ✓ Habilitación del protocolo IPv6 en el sistema de nombres de dominio de España ccTLD."es";
- ✓ Creación de un grupo de trabajo, que reúna a las organizaciones más representativas tanto público como privadas;
- ✓ Elaboración del plan de direccionamiento de las redes nacionales;
- ✓ Impulsar la incorporación de IPv6 como requisito de compra pública en productos y servicios de tecnología; y
- ✓ Encargar al MITYC y al MPTYAP, realizar el seguimiento y coordinación en el ámbito internacional.

En Marzo del 2012, España, publica el documento denominado "Guía para la incorporación de IPv6 como requisito de compra pública", en el cual se realiza un análisis de los requerimientos técnicos a tener en cuenta para la compra de hardware, software, equipo humano, comunicaciones y conectividad en las instituciones públicas de España (Públicas., 2012). El documento recomienda diversas buenas prácticas por cada componente:

- ✓ **Para hardware**, considera el uso de los 7 niveles de clasificación definidos en el RIPE-501bis, definir los RFCs requeridos y la elaboración de cuestionarios que permitan a las empresas proveedoras justificar el cumplimiento del soporte de IPv6 y de las RFC requeridas (Públicas., 2012).
- ✓ **Para el Software**, se recomienda considerar las buenas prácticas definidas por RIPE, los estándares recomendados por el

Departamento de Defensa de los Estados Unidos, realizar consultas a bases de datos especializadas en análisis de soporte IPv6 en software (6DISS – IPv6 DISSemination and Explotation, IPv6- to-Estándar, University of Wisconsin-Madison IPv6 Application Compatibility y National Information Infrastructure Development Institute), generar una lista de RFCs de cumplimiento obligatorio y exigir pruebas de funcionamiento en un ambiente doble pila (IPv4 – IPv6) (Públicas., 2012).

- ✓ **Para el equipo humano**, se recomienda que este personal disponga de alguna certificación en IPv6 con la participación en otros proyectos de tecnología (Públicas., 2012).
- ✓ **Para comunicaciones y conectividad**, se diferencia en conectividad a Internet y VPN, para cada uno de estos tipos de conectividad, se recomienda solicitar acuerdos de nivel de servicio independientes del protocolo a usarse, la no utilización de mecanismos de túneles, el 100% de tablas de enrutamiento global con IPv4 e IPv6 (Para una conectividad a Internet),

España desde el año 2002 crea el IPv6 Task Force (www.spain.ipv6tf.org), el cual tiene como objetivo la investigación sobre el nuevo protocolo IPv6 y la implementación de este en España; sin embargo, el MITYC a través del portal de administración electrónica (www.administracionelectronica.gob.es) es el que viene informando sobre la implementación del protocolo IPv6 en las instituciones públicas del gobierno de España.

En una publicación de marzo del 2013, informa que la implementación de IPv6 es del 1% y que el MPTYAP implemento el portal www.060.es (actualmente direccionado a www.administracion.gob.es), el cual es el punto de acceso para los servicios prestados a las administraciones públicas de España.

Este portal es compatible con el protocolo IPv6 y es accedido, por las administraciones públicas, a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que cumple la función de pasarela hacia la infraestructura del www.060.es. SARA es un conjunto de infraestructura de comunicaciones y servicios que conecta las redes de las administraciones públicas de España e Instituciones Europeas, para lo cual el MPTYAP y el Instituto Nacional de Tecnologías de las Comunicaciones – INTECO, vienen elaborando los borradores para la implementación total de IPv6 en la red SARA; así como también un plan de direccionamiento en IPv6 para las administraciones públicas.

En el ámbito académico, España, a través de la RedIRIS, que es la red académica y de investigación de España, participa activamente en el desarrollo y difusión de IPv6. RedIRIS, al igual que sus pares de otros países, esta interconectado con las redes avanzadas de ámbito internacional para la investigación del protocolo IPv6 y otras tecnologías (Cedia, s.f.).

La RedIRIS, publica una “Guía para el despliegue de IPv6” en instituciones que tengan un prefijo IPv4, este procedimiento se resume en los siguientes puntos (RedIRIS, s.f.):

- ✓ Solicitud de Direccionamiento.
- ✓ Solicitar el enrutamiento del prefijo.
- ✓ Configurar el DNS y pedir la delegación inversa.

- ✓ Definir un plan de direccionamiento para la institución.
- ✓ Revisar la política de seguridad.
- ✓ Revisar los procedimientos de gestión de la red.
- ✓ Actualizar los equipos de comunicaciones troncales.
- ✓ Publicar los primeros servicios con doble stack.
- ✓ Desplegar doble stack en la intranet de la organización.

Asimismo, implementa un servidor (RedIRIS) para medir y comparar la velocidad de conexión entre protocolos IPv4 e IPv6, el cual puede ser accedido a través del test de velocidad.

2.1.2 Antecedentes Nacionales

Respecto a tesis, proyectos o trabajos de investigación relacionados al tema se encontró lo siguiente:

Según (Baltazar, 2017) en su tesis titulada MODELO DE REFERENCIA DE TRANSICION DE IPv4 A IPv6 PARA EL SECTOR GOBIERNO DE PERU nos indica que la implementación de IPv6 por parte de los ISP, a nivel Perú, no ha sido generada por alguna iniciativa estratégica, regulatoria o documento normativo realizado por el gobierno peruano. Esta iniciativa corresponde al desarrollo del mercado mundial de las telecomunicaciones y principalmente al agotamiento del espacio de direcciones IPv4, lo que ha obligado a los ISP de Perú a estar preparados. Actualmente, en el Perú, los ISP ofrecen servicios de acceso a Internet con IPv6 a sus clientes residenciales y corporativos, contando con planes estratégicos de migración para sus diferentes servicios, desde los fijos a los inalámbricos. Estas acciones realizadas por los ISP en el Perú, ha permitido que el Perú sea considerado como uno de los líderes de los países que forman parte del RIR LACNIC, incluso superando en tráfico a países de

Europa; sin embargo, este liderazgo es a nivel de tráfico cursado, en mayor porcentaje por usuarios residenciales, y no representa el porcentaje de avance real de adopción de IPv6 a nivel país, específicamente por parte de las instituciones públicas o de gobierno a nivel de su infraestructura tecnológica y contenidos. Las iniciativas a nivel del gobierno peruano, para promover la adopción del nuevo protocolo, han sido casi nulas. Solo se ha encontrado un documento formal en el que se menciona el protocolo IPv6, específicamente, el documento publicado el 26 de Julio del 2011, denominado “Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0”. En este Plan, se establecen diversos objetivos a cumplirse al 2015, considerado la inclusión del protocolo IPv6. Específicamente se menciona que para alcanzar su Objetivo N° 01 “Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la sociedad de la información y del conocimiento”, deberá considerarse como estrategia lo siguiente: “Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el protocolo de Internet v6 (IPv6)”.

Tabla 1: Principales ISP con Ipv6 en el Perú

ISP	SECTOR
Telefónica del Perú	Corporativo, residencial y de telefonía móvil
América Móvil	Corporativo, residencial y de telefonía móvil
Optical Technologies	Corporativo
Viettel Perú	Residencial y telefonía móvil
Olo del Perú	Residencial y telefonía móvil
Entel del Perú	Corporativo, residencial y de telefonía móvil

Fuente: (Baltazar, 2017)

Situación Actual del NAP Perú

Conformado por los principales ISP a nivel nacional, el cual está conformada por 15 miembros, de los cuales 9 anuncian prefijos IPv4 e IPv6 a nivel del NAP.

Tabla 2: **Miembros del NAP Perú**

Nº	Miembro NAP	Versión del Protocolo en sus prefijos anunciados
1	América Móvil	IPv4/IPv6
2	Americatel Perú	Solo IPv4
3	BT Latam	IPv4/IPv6
4	Internexa	Solo IPv4
5	Level 3	IPv4/IPv6
6	Infoductos y telecomunicaciones del Perú	IPv4/IPv6
7	Media Commerce Perú	IPv4/IPv6
8	Netline Perú	Solo IPv4
9	Optical Networks	IPv4/IPv6
10	Telefónica del Perú	IPv4/IPv6
11	Telefónica Móviles	IPv4/IPv6
12	Telmex Perú	IPv4/IPv6
13	Bitel Perú	Solo IPv4
14	Entel Perú	Solo IPv4
15	Convergía Perú	No anuncia

Fuente: (Nap.pe, s.f.)

Por otro lado tenemos información casi actual, en agosto del 2017 se aprueba un decreto supremo, en el cual se indica formular un plan de transición al protocolo IPv6 en entidades públicas del estado peruano (Peruano, 2017).

Plazo

En el cual se indica que todas las entidades públicas del estado tienen un plazo máximo de 1 año para realizar sus planes correspondientes y hasta 4 años adicionales para su implementación, cabe resaltar que el tiempo es de referencia, se debe indicar también que se la infraestructura tecnológica actual en muchas entidades públicas del país no soportarían este cambio al ser obsoletas, por tanto estos 4 años siguientes se tendrían que realizar cambios a nivel de hardware, realizar planes de contingencia para así poder tener una correcta implementación hacia el protocolo Ipv6.

Estrategia para la implementación del protocolo IPv6 del Estado Peruano

La Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros en coordinación con los actores pertinentes desarrollará las acciones necesarias (lineamientos, guías, proyectos, capacitaciones, otros) para la adecuada implementación del protocolo IPv6 (Peruano, 2017).

Implementación del protocolo IPv6 en los Gobiernos Locales

Los Gobiernos Locales fuera del alcance del presente Decreto Supremo, que en función de sus capacidades técnicas, infraestructura tecnológica, acceso al servicio de Internet podrán elaborar su Plan de Transición al Protocolo IPv6, en base a lo estipulado en el presente Decreto Supremo, y atendiendo a la Estrategia para la implementación del protocolo IPv6 en el Estado Peruano (Peruano, 2017).

2.2 Bases teóricas

2.2.1 Modelo OSI

El modelo de interconexión de sistemas abiertos u OSI, por sus siglas en inglés (Open Systems Interconnection), es un modelo estructurado en capas para los protocolos en red, que tiene como finalidad generar un lineamiento para el intercambio de información entre equipos informáticos.

En esta arquitectura, tal como describe (Tomasi W. , 2003), se separan las responsabilidades de la red en siete capas distintas, estratificando dichas responsabilidades de manera que, cada capa añada valores a los servicios suministrados por los conjuntos de las capas inferiores, siendo el nivel más alto quién cuenta con todos los servicios necesarios para el funcionamiento de una aplicación de datos distribuidos.

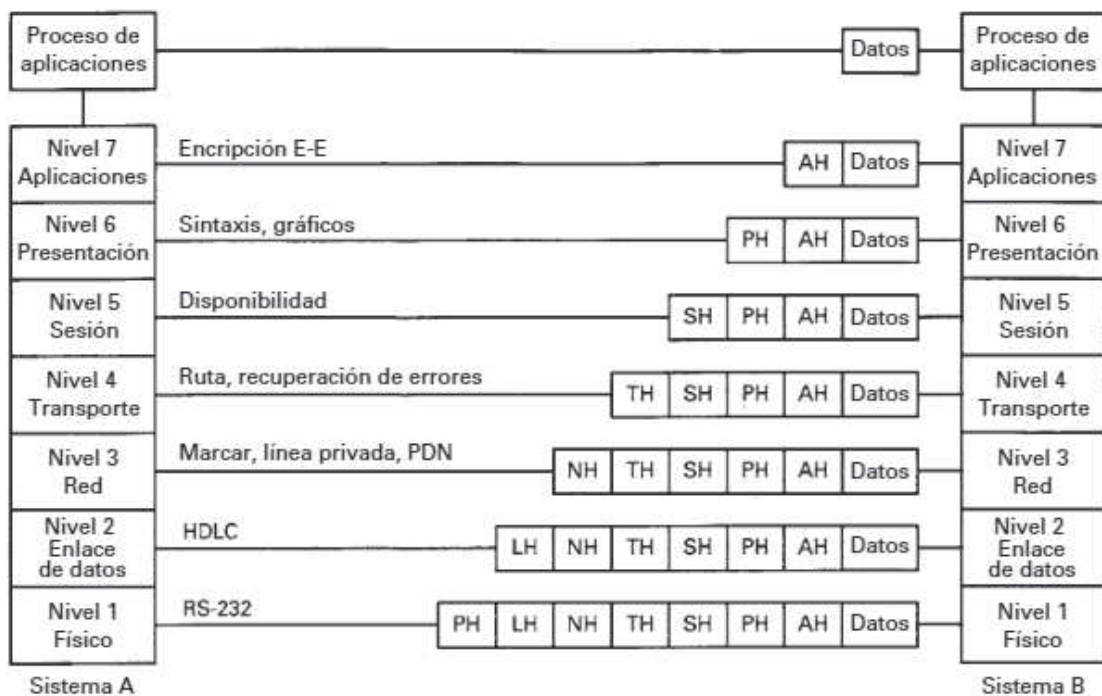


Figura 1: Modelo OSI

Fuente: (Tomasi W. , 2003)

2.2.2 Redes de Computadoras

Es un conjunto de computadoras que van a compartir archivos (carpetas, datos, imágenes, audio, video, etc.) o recursos (disco duro, lectora, disquetera, monitor, impresora, fotocopidora, web cam, etc.), estas computadoras pueden estar interconectadas por un medio físico o inalámbrico.

2.2.3 Medios de transmisión

La transmisión de datos en una red de computadoras se produce a través de un medio de transmisión o combinación de distintos medios como son:

➤ Cable de par Trenzado

Consta de dos cables de cobre aislados, por lo general de 1 mm de grosor. Los cables están trenzados en forma helicoidal, justo igual que una molécula de ADN. La aplicación más común del par trenzado es el sistema telefónico. Casi todos los teléfonos se conectan a la central telefónica mediante un par trenzado (Tanenbaum, 2015).

➤ Cable coaxial

Es otro medio de transmisión común conocido también como “coax”, este cable tiene un mejor blindaje y mayor ancho de banda que los pares trenzados, por lo que abarca mayores distancias a velocidades más altas (Tanenbaum, 2015). Se lo utiliza más para la televisión por cable, y también para alguna transmisión analógica o digital.

➤ Fibra óptica

Este medio funciona a través de luz óptica y utiliza para la transmisión datos e internet de larga distancia en las redes troncales que abarca hasta altas velocidades y ancho de banda su principal competidor es el cable de cobre, ya

que se le ha podido poner a la par, pero por varias ventajas lo supera la fibra óptica.

➤ Internet

Luego de haber comprendido lo que es una red de computadoras y cuáles son los medios de transmisión físicos por donde viajan los datos o el término que el usuario común conoce como Internet, todo esto es gracias al INTERNET que proviene de Interconneted Networks que significa Redes Interconectadas, lo cual básicamente se trata de millones de computadoras conectas entre sí en una red mundial.

Su forma de operación es descentralizada, esto significa que la información no necesita pasar necesariamente por un nodo de la red, sino que puede tomar caminos alternativos según convenga (definicionabc.com, 2015). Sus orígenes remontan desde 1969 cuando se estableció la primera conexión de computadoras, conocida como ARPANET entre tres Universidades en California.

2.2.4 Direccionamiento IP

En una red de comunicación de datos, cada dispositivo debe tener una identificación o una dirección que debe ser única en la red. Esta identificación se le llama dirección IP. Este número en el protocolo IPv4 está dividido en cuatro octetos de ocho bits cada uno separados por puntos y puede tener un valor de 0 a 255.

Hay dos maneras de asignar estas direcciones:

De forma fija

Se hace mediante configuración manual por parte del usuario mediante un software, se utiliza en algunos ordenadores que tienen alguna relevancia en la red.

De forma dinámica

Se hace por medio de un enrutador capaz de entregar direcciones IP de forma dinámica o automática, mediante la función DHCP (Martin, 2010). Las direcciones ip son esenciales para determinar la asignación que se debe hacer en los routers de borde que deben tener los dos protocolos conviviendo en una misma red.

2.2.5 Protocolos de comunicaciones

Hace algunos años cuando se empezaron a crear las redes de computadores, los fabricantes de los ordenadores empezaron a desarrollar sus propios terminales, cada uno con sus respectivos software y hardware. Es así como OSI (International Organization for Standarization) trato de estandarizar y normalizar las reglas con que los equipos de diferente fabricante se pudieran conectar.

Los protocolos de comunicaciones son un grupo de normas para la transmisión y recepción de datos entre dos nodos de una red. Las condiciones de comunicación se hacen mediante un proceso llamado acuerdo de conexión. Para generar la trasferencia y recepción de los archivos los dos dispositivos deben tener un protocolo que ambos puedan gestionar. La finalidad de estas normas es fijar unos parámetros para codificar y decodificar los datos señalizando los paquetes que son la forma como la información se embala para poder transferir

a través de una red a donde se deben enviar y reduciendo las probabilidades de un ataque a la información (June Parsons, 2008).

2.2.6 Protocolo de internet

Es una serie de normas o leyes que se basan en internet y que permite la trasmisión entre ordenadores. Los primeros en ser definidos fueron el TCP/IP, TCP y el protocolo IP. Existen muchos protocolos de internet que se relacionan con el internet como el HTTP que se utiliza para entrar a las páginas de internet, y otros como ARP para la resolución de direcciones, el FTP para la transferencia de archivos y el TELNET para acceder a equipos remotos. Estos protocolos están definidos por el modelo OSI (Open System Interconnection) que describe que se necesitan para poder establecer la conexión entre dos dispositivos en una red (Yair Duran, 2010).

2.2.7 IPv4

Se creó a principios de los años 80's, es la primera versión oficial de direccionamiento IP que permite identificar a un dispositivo mediante una dirección única en la red. El modelo contemplado en este formato es de 4 octetos de 8bits cada uno, para un total de 32 bits con lo que no puede entregar un poco menos de 4300 millones de ubicaciones. (L.M, 2012)



Figura 2: Datagrama IPv4

Fuente: (Montes, 2005)

El campo versión lleva el registro de la versión del protocolo al que pertenece el datagrama. Al incluir la versión en cada datagrama es posible hacer que la transición entre versiones se lleve meses, o inclusive años (neo.lcc.uma.es, s.f.).

La longitud de la cabecera no es constante, por eso se incluye un campo en la cabecera IHL para indicar la longitud en palabras de 32 bits. El campo tipo de servicio permite al host indicar a la subred el tipo de servicio que quiere. Son posibles varias combinaciones de confiabilidad y velocidad. El campo mismo contiene (de izquierda a derecha) un campo de precedencia; tres indicadores, D,T y R; y 2 bits no usados. El campo de precedencia es una prioridad, de 0 (normal) a 7 (paquete de control de red). Los tres bits indicadores permiten al host especificar lo que le interesa más del grupo (retardo, rendimiento, confiabilidad) (neo.lcc.uma.es, s.f.)

La longitud total incluye todo el datagrama: tanto la cabecera como los datos. La longitud máxima es de 65535 bytes. El campo identificación es necesario para que el host destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación (neo.lcc.uma.es, s.f.).

Luego viene un bit sin uso, y luego dos campos de 1 bit. DF significa no fragmentar, y MF significa más fragmentos. El desplazamiento del fragmento indica en qué parte del datagrama actual va este fragmento. Todos los fragmentos excepto el último del datagrama deben tener un múltiplo de 8 bytes que es la unidad de fragmento elemental. El campo tiempo de vida es un contador que sirve para limitar la vida del paquete. El campo protocolo indica la capa de transporte a la que debe entregarse (TCP o UDP o algún otro). La suma

de comprobación de la cabecera verifica solamente a la cabecera (neo.lcc.uma.es, s.f.).

El campo opciones se rellena para completar múltiplos de cuatro bytes. Actualmente hay cinco opciones definidas, aunque no todos los encaminadores las reconocen: Seguridad, Enrutamiento estricto desde el origen, Enrutamiento libre desde el origen, Registrar ruta y Marca de tiempo (neo.lcc.uma.es, s.f.).

2.2.8 IPv6

La versión 6 del protocolo IP es la unión de trabajos encaminados por la IETF (Internet Engineering Task Force) desarrollado en 1994; Una dirección IPv6 es un número binario de 128 bits y se representan en 8 grupos de 4 dígitos hexadecimales separados por dos puntos ":" con la cual ofrece una cantidad de direcciones suficientes para el crecimiento y evolución de redes futuras. Sus principales mejoras con respecto al protocolo anterior son la disminución de campos en el encabezado, mayor posibilidad de conexión y flexibilidad global, optimización de agrupación de los prefijos IPv6 para las tablas de enrutamiento, terminales con múltiples conexiones, procesos de autenticación y seguridad con el protocolo de seguridad IPSec el cual ya viene embebido en el protocolo (Paiola, 2016).

Versión	Clase del tráfico	Etiqueta del flujo	
Longitud de la carga útil		Jefe siguiente ⁴⁸⁻⁵⁵	Límite del salto
Dirección de fuente			
Dirección de destino			

Figura 3: Datagrama IPv6

Fuente: (6sos.org, 2004)

Versión (4 bits): representa la versión del Protocolo de Internet, es decir 0110. Espacio de 8 bits que indican las necesidades del tráfico del paquete. Clase de Tráfico (8 bits), Estos 8 bits se divide en dos partes, los más importantes 6 bits se utilizan para el tipo de servicio para que el Router sabe qué servicios deben ser proporcionados a este paquete. Los 2 bits menos significativos se utilizan para Notificación de congestión explícita (ECN). La etiqueta de flujo (20 bits); Esta etiqueta se usa para mantener el flujo secuencial de los paquetes pertenecientes a la comunicación. Las etiquetas de fuentes la secuencia para ayudar a identificar el router que un paquete en particular pertenece a un determinado flujo de información. Este campo permite evitar un reordenamiento de paquetes de datos. Está diseñado para la transmisión/multimedia en tiempo real (Learning, 2016).

Payload Length (16 bits); Este campo se utiliza para indicar a los routers la cantidad de información contiene un paquete en particular en su capacidad de carga. El paquete está compuesto por extensión Los encabezados y los datos de la capa superior. Con 16 bits, hasta 65535 bytes pueden ser indicadas, pero si la extensión los encabezados incluyen salto por salto Extensión del cabezal, a continuación, la carga útil puede exceder 65535 bytes y el valor de este campo se establece en 0 (Learning, 2016).

Next Header (8 bits); Este campo se utiliza para indicar el tipo de extensión del cabezal, o si la extensión del cabezal no está presente, entonces indica la capa superior PDU. Los valores para el tipo de capa superior PDU son los mismos que IPv4 's. Hop Limit (8 bits); Este campo se utiliza para detener paquete en forma de bucle en la red infinitamente. Esta es la misma que TTL en IPv4. El valor de Límite de Salto se decrementa en 1, que pasa a través de un

enlace (router/salto). Cuando el campo llega a 0 se descarta el paquete. Dirección de origen (128 bits); Este campo indica la dirección de origen del paquete; y por último Dirección de Destino (128 bits); Este campo proporciona la dirección de destinatario del paquete (Learning, 2016).

Además, tiene un tipo de direcciones específicas las cuales nos dan un servicio distinto para cada una; las direcciones unicast se caracteriza por identificar un único punto final de destino. Un datagrama enviado a una dirección Unicast será entregado a un solo punto de destino; las multicasts son tipos de direcciones agrupan un conjunto de puntos finales de destino. Un datagrama enviado a una dirección multicast será entregado a un conjunto de destino que forman parte de un mismo grupo y por último las anycast que también agrupan un conjunto de puntos finales, pero a diferencia de multicasts, anycast tiene un sistema diferente para la entrega de datagramas.

Para el caso de IPv6 se definieron tres tipos de direcciones:

Unicast:

Este grupo de direcciones se caracteriza por identificar un único punto final de destino. Un datagrama enviado a una dirección unicast será entregado a un solo punto de destino.

Todas las interfaces están obligados a tener al menos un enlace local unicast Una única interfaz puede tener múltiples direcciones IPv6 de cualquier tipo (unicast, anycast y multicast) o ámbito de aplicación. Una dirección unicast o un conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas si la aplicación trata de la múltiple interface física como una única interfaz cuando se presentan a la capa de Internet. Esto es útil para el intercambio de carga sobre múltiples interfaces físicas.

Actualmente, IPv6 sigue el modelo de IPv4 en que un prefijo de subred es asociado con un enlace. Varios prefijos de subred se le pueden asignar en el mismo enlace.

Su estructura es como se indica en este grafico



Figura 4: Formato dirección Unicast

Multicast

Un identificador para un conjunto de interfaces (típicamente pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificada por esa dirección. Las direcciones IPv6 "multicast" tienen la estructura presentada en la Figura 4.

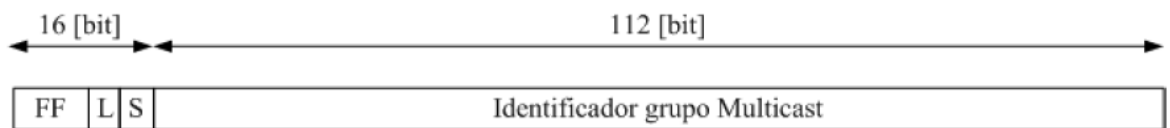


Figura 5: Dirección Multicast

El campo L indica el tiempo de vida de un grupo "multicast", tomando el valor de 0 cuando es un grupo permanente y 1 cuando es un grupo "multicast" temporal. El campo S indica el contexto o alcance del grupo, de acuerdo con los valores presentados en la figura siguiente.

Anycast

Una dirección IPv6 anycast es una dirección que se asigna a más de una interfaz (típicamente pertenecientes a diferentes nodos), con la propiedad de que un paquete enviado a una dirección anycast se encamina a la "Más cercana" de las interfaces que tiene que abordar, de acuerdo con la hoja de ruta protocolos de medida de la distancia. Las direcciones Anycast se asignan desde el espacio

de direcciones unicast, usando cualquiera de los formatos definidos dirección unicast. Por lo tanto, las direcciones anycast son sintácticamente indistinguibles de las direcciones unicast. Para cualquier dirección anycast asignada, existe un prefijo más largo de que dirección que identifica la región topológica en el que todas las interfaces que pertenecen a esa dirección anycast que residen. Dentro de la región identificada por P, la dirección anycast debe mantenerse como una entrada separada en el sistema de encaminamiento (comúnmente conocido como un huésped. En ese caso, la dirección anycast debe mantenerse como una entrada independiente de enrutamiento a través de Internet, que presenta una grave ampliación límite sobre el número de tales grupos "globales" anycast pueden ser compatible. Por lo tanto, se espera que el apoyo a anycast mundial conjuntos pueden no estar disponibles o muy restringida. El "prefijo de subred" en una dirección anycast es el prefijo que identifica a un enlace específico. Esta dirección anycast es sintácticamente lo mismo que una dirección unicast para una interfaz en el enlace con el identificador de interfaz pone a cero.

2.2.9 Comparación entre los protocolos IPv4 e IPv6

Para entender los beneficios de una posible transición del protocolo IPv4 a IPv6, es necesario realizar una comparación detallada sobre los principales conceptos y características, con el fin de obtener un conocimiento más profundo sobre las particularidades de los protocolos.

De esta manera y tomando como base los contenidos presentados en (IBM Knowledge Center, s.f.), en donde se realiza una comparación entre 54 tópicos principales, se procederá a realizar una recopilación breve de los aspectos fundamentales de algunos de estos tópicos que generarán el contexto adecuado para posterior análisis y conclusión.

2.2.9.1 Dirección

El protocolo IPv4 establece un conjunto de direcciones IP de longitud de 32 bits (4 bytes), en el que la dirección está estructurada como una parte de red y una parte de sistema principal, siendo dichas partes establecidas de acuerdo a la clasificación de la dirección, ya sea A, B, C, D o E, según el número de bits iniciales; por tanto, el número total de direcciones IPv4 que se puede generar es de un total de 4.294.967.296.

En contraparte, el protocolo IPv6, realiza un aumento en la longitud de la dirección, llegando a 128 bits (16 bytes), basándose en una arquitectura diferente, en donde se plantea 64 bits para el número de red y 64 bits para el número de sistema principal o host. Cabe recalcar que el número de direcciones IPv6 es de un total de 2128.

Así, se tiene que el protocolo IPv6 aumenta 79.228.162.514.264.337.593.543.950.336 veces, el número de posibles direcciones IP que se pueden generar con el protocolo IPv4.

2.2.9.2 Asignación de direcciones

Para el protocolo IPv4, se realiza un proceso de asignación por clase de red, esto se traduce en una asignación que depende de la demanda de direcciones, en tanto tenga un aumento, y en consecuencia se agote el espacio de direcciones, se realizan asignaciones más pequeñas.

Por el contrario, para el protocolo IPv6 se realiza un proceso de asignación en el que se recomienda asignar una longitud de prefijo /48, para cualquier tipo de entidad, ya sea una organización, un domicilio privado o demás. Lo cual, a su vez expresa, una política de asignación de 16 bits para división en subredes para la organización.

2.2.9.3 Máscara de dirección

En el protocolo IPv4, la máscara de dirección se utiliza con la finalidad de designar la red desde la parte del sistema principal, sin embargo, en el protocolo IPv6 dicha máscara de dirección no se utiliza.

2.2.9.4 Prefijo de la dirección

En el protocolo IPv4, el prefijo de la dirección, es utilizado, al igual que la máscara de dirección, para diferenciar la red de la parte del sistema principal o host, en donde puede escribirse como sufijo (/nn), de máximo dos dígitos, en el formato de presentación de la dirección.

Por otra parte, el prefijo de la dirección, en el protocolo IPv6, se utiliza para designar el prefijo de subred, en donde y al igual que en el protocolo IPv4, se escribe como sufijo (/nnn), de máximo tres dígitos, en el formato de impresión de la dirección.

2.2.9.5 ARP

El protocolo ARP está presente en el direccionamiento IPv4, siendo el responsable de encontrar la dirección MAC, de una dirección ipv4, por medio de envíos de paquetes, también llamados ARP Request, a la dirección broadcast de la dirección IPv4.

Por otra parte, en el IPv6, las funciones del protocolo ARP se incrustan desde de sí mismo, como parte de los algoritmos para autoconfiguración sin estado y descubrimiento del vecino.

2.2.9.6 Configuración

El protocolo IPv4 exige que se realice la configuración del sistema para que pueda establecer la comunicación con otros sistemas, refiriéndose al tema de asignación de rutas, en conjunto con las direcciones IP.

Sin embargo, en el protocolo IPv6, se encuentra un contexto distinto, en donde la configuración es opcional, y se adecúa a las funciones que se requieren. Este protocolo, permite que las interfaces IPv6 puedan utilizar una configuración automática, utilizando una autoconfiguración sin estado de IPv6; a la par de permitir la realización de una configuración manual de la interfaz IPv6.

2.2.9.7 Fragmentos

En el protocolo IPv4, se puede presentar un proceso de fragmentación del paquete, ya sea desde el sistema principal o direccionador, cuando dicho paquete es demasiado grande para el enlace por el que debe viajar, presentando esto problemas, con respecto a la duplicación de fragmentos, e incluso en el orden de dichos fragmentos.

Por otra parte, en el protocolo IPv6, se encuentra con que la fragmentación es un proceso que se realiza únicamente desde su envío en el nodo origen, y es reensamblado sólo en el nodo destino.

2.2.9.8 Cabecera IP

De acuerdo a la necesidad de fragmentación de paquetes IP, se tiene de igual manera la necesidad de reensamblar dichos paquetes, siendo en este caso la cabecera, la que juega un papel fundamental en este proceso. es entonces, la que almacena el identificador del fragmento, es decir el identificador único para el posterior reensamblaje, además de la información referente a su orden en el paquete final, el tamaño de los datos que se transportan en el fragmento y el valor que indica si es el último fragmento o no.

Así, en IPv4, la longitud de la cabecera tiene una longitud variable, de entre 20 a 60 bytes, contra una longitud fija de 40 bytes, en el caso del protocolo IPv6.

2.2.9.9 Direcciones privadas y públicas

En el direccionamiento IPv4, todas las direcciones IP presentes, son públicas, exceptuando tres intervalos de direcciones que se han designado como privadas (10/8, 172.16/12 y 192.168/16), en donde por lo general, dichas direcciones privadas son utilizadas para para los sistemas de las redes locales de una intranet corporativa, teniendo la particularidad de no poder ser direccionadas a través de internet.

Por el contrario, y aunque en IPv6 se maneja un concepto similar, dado que se encuentran también direcciones públicas, se crea el concepto de dirección temporal, las cuales y a diferencia de las direcciones privadas en el protocolo IPv4, pueden ser direccionadas globalmente y generalmente no

pueden ser distinguidas de una dirección pública normal; esto a la par de tener un enfoque muy distinto, ya que buscan la protección de la identidad de un cliente, dado que tienen un tiempo de vida limitado y no contienen un identificador de dirección que sea una dirección de enlace MAC.

2.2.9.10 Cambio de numeración

En el protocolo IPv4, es un proceso efectuado mediante una nueva configuración manual, con la posible excepción de DHCP. Comúnmente, este es un proceso difícil y problemático, y por tanto debe evitarse siempre que se pueda.

Sin embargo, esto es algo completamente distinto en el protocolo ipv6, en donde este proceso es un elemento arquitectónico importante de dicho protocolo, siendo en gran parte automático.

2.2.10 Beneficios de la transición de IPv4 a IPv6

Según (MINTIC., 2011) y de acuerdo a lo que se enuncia en las secciones anteriores, existen varios beneficios que pueden surgir de la transición del protocolo IPv4 a IPv6. A continuación se presentarán algunas de ellos:

- Capacidad de conexión a un mayor número de dispositivos a la red.
- Transparencia para los usuarios finales, tanto en sus comunicaciones, servicios, aplicaciones y demás.
- Mejora en la seguridad a nivel del direccionamiento IP, dada la arquitectura del nuevo protocolo.
- Aumento en la cantidad de direcciones IP accesibles en la entidad.
- Según (LACNIC, IPv6: “mientras más tiempo pase, más recursos tendrán que invertir”, s.f.), la transición al protocolo IPv6 por parte de las entidades puede resultar más rentable, que postergar el proceso.
- Acompañamiento por parte de los proveedores de servicio, quienes tendrán que realizar la transición de dichos servicios, apoyando en el proceso de enrutamiento de las direcciones IPv6.
- Capacidad de adopción y apertura a nuevas tecnologías como el internet de las cosas, las ciudades inteligentes, redes de sensores, entre otras.
- Facilitará la conectividad en banda ancha.

2.2.11 Mecanismos de transición

En medio del proceso de transición del protocolo IPv4 al protocolo IPv6, debe entenderse que el protocolo IPv4 aún está vigente, e incluso existen ciertas tecnologías incompatibles con el protocolo IPv6. Dado lo anterior existen métodos de transición que buscan la coexistencia de redes IPv4 con los despliegues del protocolo IPv6.

Lo anterior, retomando el esfuerzo del Grupo de Trabajo de Transición a IPng, por parte de la IETF, y entendiendo que uno de los pilares del diseño del protocolo IPv6, como lo expresa (LACNIC, Mecanismos de transición, s.f.), fue precisamente la realización de una transición que pudiera llevarse a cabo de forma paulatina y gradual, es decir, sin que sea necesario el paso a de IPv4 a IPv6 de forma abrupta. Por tanto, se han diseñado diversos protocolos, herramientas y mecanismos como soporte al proceso de transición del protocolo IPv4 a IPv6, que permita la convivencia o coexistencia de ambos protocolos.

Gracias a esto, se pueden encontrar tres estrategias principales, diseñadas específicamente para dicho proceso de transición:

- Doble pila (Dual stack).
- Túneles.
- Traducción.

Tunelización:

Proporciona una manera de utilizar la infraestructura de IPv4 para llevar el tráfico IPv6. Una de las principales características más importantes es la compatibilidad existente entre los dos protocolos mientras que se puede desplegar completamente IPv6. Se pueden establecer túneles de datagramas IPv6 a través de topologías pertinentes a IPv4 encapsulándolos en datagramas IPv4 (IBM, s.f.).

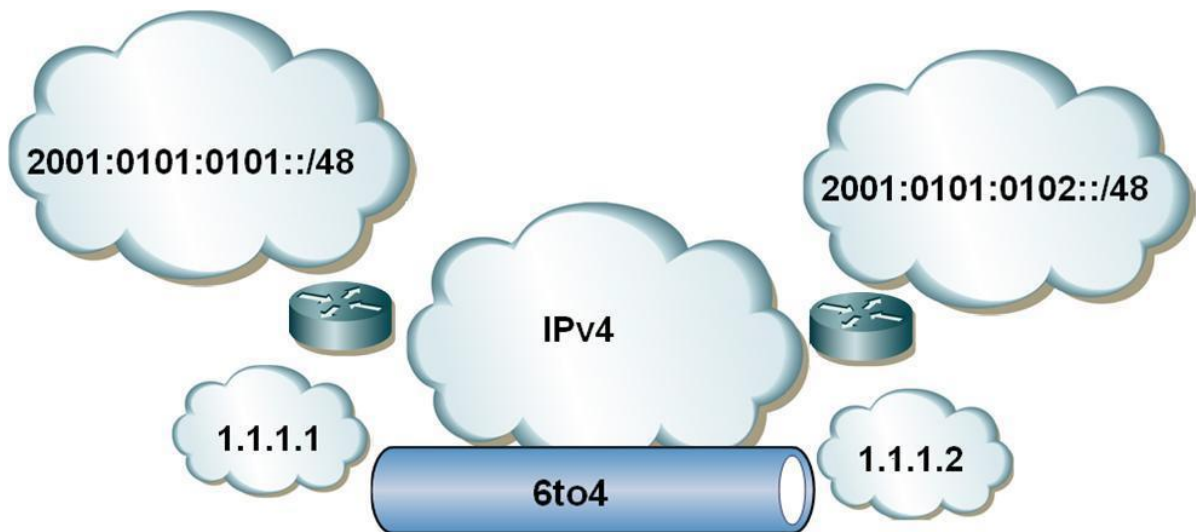


Figura 6: Tunelización IPv6 a IPv4

Fuente: (IBM, s.f.)

Dual Stack:

Este método de transición propone mantener dos pilas de protocolo los cuales trabajan paralelamente para que se permita a los dispositivos de la red trabajar sobre los dos protocolos. En este sistema se deben tener unos requerimientos del sistema efectivo y capaz de poder procesar la información para los dos protocolos ya que tienen que tener un doble procesamiento, efectuando las distintas aplicaciones que corren sobre IPv4 e IPv6. Estos sistemas generalmente trabajan por defecto con IPv6 para comunicarse con sistemas iguales y al mismo tiempo pueden retroceder utilizando IPv4. Los nodos que contienen este método tienen que tener los dos protocolos activados y trabajará dependiendo del flujo que se basa en el encabezado IP (Americas).

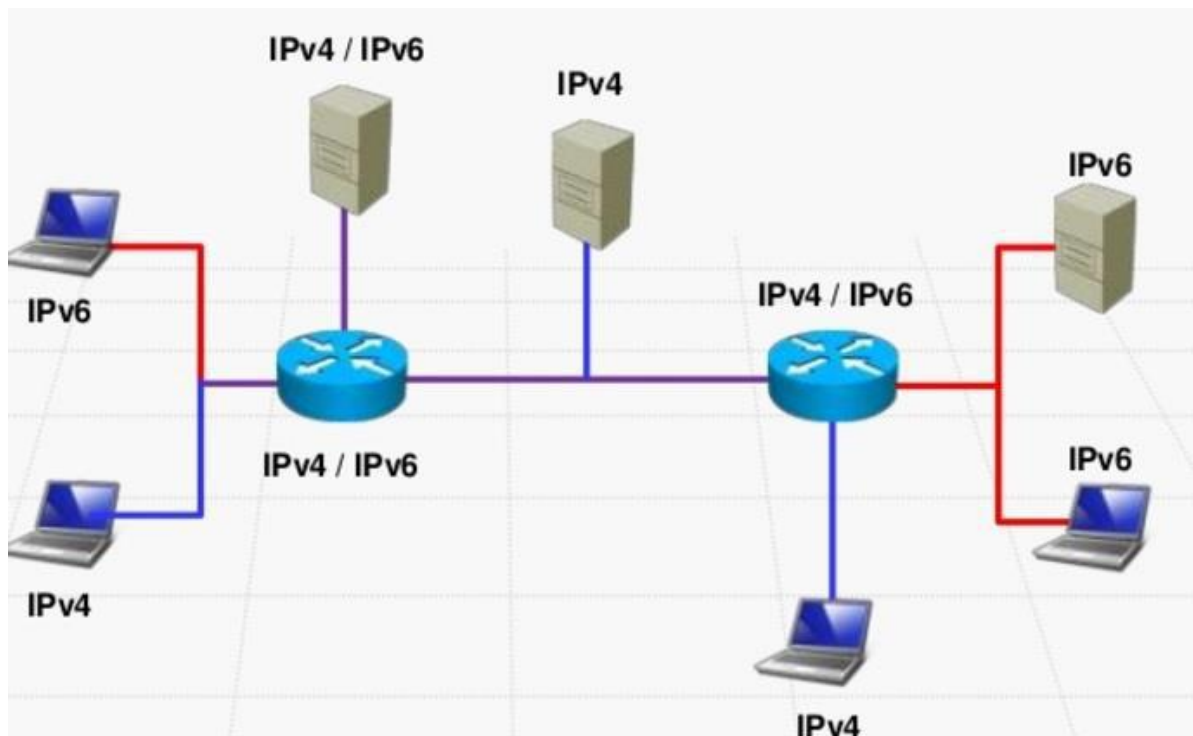


Figura 7: Método Dual Stack

Fuente: (Garometta, 2012)

Método de traducción:

Se refiere específicamente a una traducción directa de la dirección en el formato de IPv4 al formato de la IPv6, de manera bidireccional y puede transformar el encabezado como de la carga efectiva del protocolo. Este mecanismo se puede utilizar en varias capas del modelo OSI. En este proceso de traducción la detección del camino MTU es mandatorio para IPv6, pero opcional para IPv4; lo que conlleva a que la fragmentación de los paquetes se haga desde el nodo fuente y se especifique en el nuevo encabezado IPv6 (Americas).

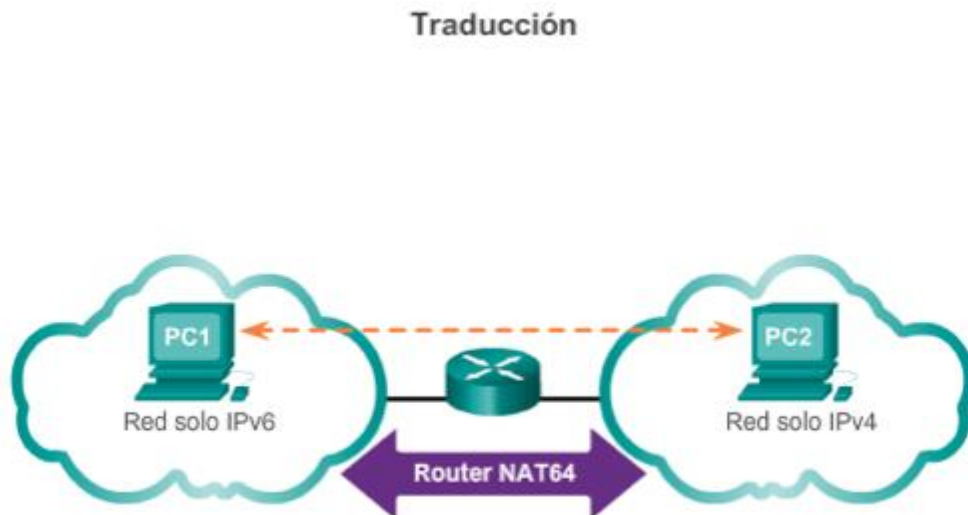


Figura 8: Método de Traducción

Fuente: (sites, 2012)

2.3 Definición de términos básicos

IANA (Internet Assigned Number Authority). La Agencia de Asignación de Números Internet era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

IP (PROTOCOLO DE INTERNET): Soporte lógico básico empleado para controlar sistemas de redes. Este protocolo especifica cómo las computadoras de puerta encaminan la información desde el ordenador emisor hasta el ordenador receptor.

ARPA: (Agencia de Investigación de Proyectos avanzada) Organización de Estados Unidos dedicada al desarrollo de las primeras redes de ordenadores (Guazmayan, 2004).

ARPANET: Nombre dado a la primera red de comunicación de ordenadores desarrollada por el ARPA para organismos gubernamentales y de investigación que transmitió por primera vez los datos en forma de paquetes (McLeod, 2000).

Banda Ancha: Es un servicio o sistema que necesita canales de transmisión capaces de superar tasas superiores a 2 Mbps (Xavier Hesselbach, 2002).

DHCP (Dynamic Host Configuration Protocol): Es un protocolo de red que permite a los usuarios de una red IP obtener los parámetros de configuración automáticamente (Mathom, 2004).

FTP: Permite la conexión a cualquier usuario en una red, emplea la clasificación de un archivo binario para todos los archivos que no son de texto. Utiliza 58 comandos independientes, aunque el usuario solo necesita saber 3 comandos básicos (Herrera, 2003).

Host: Es una computadora que mediante la utilización de protocolos TCP/IP permite a los usuarios comunicarse con otros sistemas (Bernardini, 2005).

HTTPS: (Hypertext Transfer Protocol) es el protocolo en cada transacción que se hace en WWW (Word Wide Web). Define la semántica que utilizan los elementos de software de la arquitectura Web (Bernardini, 2005).

IBM: (International Business Machines) empresa multinacional de Estados Unidos dedicada a la comercialización de hardware y software de computadoras.

IETF: (Internet Engineering Task Force) Es un grupo de trabajo de ingenieros que se encarga de establecer los requerimientos y protocolos necesarios para las aplicaciones o de movilidad IP (Benjamin Ramos Alvarez, 2004).

Internet: red de redes interconectadas a nivel mundial legisladas por una serie de protocolos con la particularidad de que cada una es independiente y autónoma (Juncar, 2001).

Paquete de Datos: Es la unidad básica para transferir datos mediante el protocolo TCP/IP conectados entre dispositivos electrónicos. Es una estructura que tiene una parte de cabecera, otra parte central de información y una cola que permite reconocer donde está el inicio y el fin del paquete (Guazmáyan, 2004).

Red de comunicaciones: Es un conjunto de elementos que proporcionan la conexión constante entre todos los usuarios que pueden actuar en una red determinada. Estas redes se dividen en públicas y privadas entregando una óptima calidad para ofrecer datos, voz y video (Moya, 2006).

PAN (Personal Área Network): Es una red de área personal, proporciona un medio de comunicación inalámbrica dentro de una red LAN, como dentro de una oficina, salón, o alcoba (ED.AL, 2003).

LAN (Local Area Network): Es la manera más básica de generar una comunicación de datos de propiedad privada, en el que los usuarios comparten recursos e información entre la gran variedad de dispositivos que estén en ella. Proporciona comunicación en los dos sentidos en un área geográficamente limitada (Tomasi W. , 2003).

MAN (Metropolitan Area Network): Es una red digital orientada al dominio público basado en aplicaciones públicas con acceso compartido que se pueden conectar con otras redes MAN y que está conformada por varias redes LAN (ED.AL, 2003).

WAN (Wide Area Network): Es una red donde la cobertura puede llegar a ser continental, une varias redes MAN. Son construidas por organizaciones privadas y brinda una conexión con gran velocidad. Pueden comunicarse vía radioenlace o satelital (McLeod, 2000).

CAPITULO III: DESARROLLO DEL OBJETIVO DE SUFICIENCIA

3.1 Situación actual de BP SUPPORT

Actualmente en la empresa se manejan un gran número de equipos, los cuales son los siguientes:

- 1 L3 Fortigate 300D
- 1 CISCO 3560G TS 48 Ports #CORE
- 2 Switch Gigabit TEG 448WS 48 Port Ethernet 4 Port SFP
- 3 Switch Trendnet Web Smart Gigabit Switch TEG 240WS 24 Port
- 1 Switch Trendnet Web Smart Gigabit Switch TEG 160WS 16 Port
- 1 Switch TP-Link TL SG1024D 24 Port Gigabit Switch
- 1 NVR Hikvision
- 1 PBX DENWA
- 5 Unifi AP

Cada equipo mencionado tiene su respectiva función en el Datacenter que se administra en la sede, para nosotros los más importantes resaltan el equipo que nos brinda seguridad perimetral (Fortigate) y el equipo CISCO 3560 que nos brinda internet a la agencia.

En el ANEXO A, se muestra una pequeña fracción del equipo principal el “core” de la empresa, el cual nos brinda internet y actualmente se encuentra administrado por nosotros.

Con el fin de realizar la migración se tiene que tener conocimientos intermedios para hacer las gestiones correspondientes en el equipo principal, vale decir que se tiene que agregar ciertos parámetros mediante la interfaz de líneas de comando en el router y este sea administrado de la mejor manera.

Esta implementación se debe realizar de manera progresiva, en las pruebas que se detallan más adelante el más óptimo de los métodos es dual Stack, por su simplicidad y rapidez para lograr el objetivo planteado la migración hacia el protocolo de internet 6.

Como parte del proceso de implementación se tomó como referencia una pequeña parte de la red interna de la empresa BP SUPPORT, en el ANEXO B, se encuentra detallado todo el diagrama de red el cual contiene los equipos router, switch, servidor de controlador de dominio (Active Directory), servidor de controlador Unifi (Acces Point), la seguridad perimetral (Fortigate), entre otros.

Para ello se hizo uso del aplicativo llamado Packet Tracer en su versión 7.0, el cual fue de mucha ayuda para hacer estas pruebas con routers y equipos que se encuentran en la red de la empresa.

Tabla 3: **Direccionamiento de clientes y servidores**

Nombre del dispositivo	Dirección IP	Puerta de enlace (Gateway)
PC0	10.1.1.2/24	10.1.1.1
PC1	2001: 1: 1: 1 :: 2/64	2001: 1: 1: 1 :: 1
R1-E0 / 0	10.1.1.1/24	N / A
R1-E0 / 1	2001: 1: 1: 1 :: 1/64	N / A
R1-S0 / 0/0	10.2.2.1/24	N / A
R1-S0 / 0/0	2001: 2: 2: 2 :: 1/64	N / A
R2-S0 / 0/0	10.2.2.2/24	N / A
R2-S0 / 0/0	2001: 2: 2: 2 :: 2/64	N / A
R2-E0 / 0	10.3.3.1/24	N / A
R2-E0 / 0	2001: 3: 3: 3 :: 1/64	N / A
Servidor	10.3.3.2/24	10.3.3.1
Servidor	2001: 3: 3: 3 :: 2/64	2001: 3: 3: 3 :: 1

Fuente: Elaboración propia

3.2 Modelo de transición del protocolo IPv4 a IPv6

Como parte de la transición del protocolo IPv4 a IPv6, se presentará un modelo inicial, por tanto y de acuerdo a lo presentado, a continuación, se presentarán las tres fases principales de la transición.

3.2.1 Fase de planeación de IPv6

La fase de planeación, es una etapa crítica en el proceso de transición, dado que debe realizarse cuidadosamente, para tener claro todos los aspectos técnicos, de infraestructura y demás, que harán parte del proceso y pueden afectar a la posterior implantación de los cambios a realizar. De esta manera, se llevarán a cabo, las siguientes actividades que son descritas en:

- Identificación de la topología actual de la red y su funcionamiento dentro de la organización, generando una propuesta para un nuevo diseño de dicha red sobre IPv6.
- Identificación de la configuración y los esquemas de seguridad de la red de comunicaciones y sistemas de información.
- Revisión de las políticas de enrutamiento para IPv6, en los segmentos de red internos, de tal manera que el tráfico presente en ella, esté plenamente controlado, desde el firewall respectivo de la entidad.
- Establecimiento del protocolo de pruebas de validación para aplicativos, equipos de comunicaciones, equipos de cómputo y demás, realizando a su vez, la planeación correspondiente a la ejecución y configuración de pruebas piloto de IPv6, analizando el comportamiento de cada dispositivo de la red de comunicaciones.

- Realización de capacitaciones a funcionarios pertenecientes a las áreas o departamentos de TI, en la entidad, y el establecimiento de campañas de sensibilización sobre el nivel de impacto del nuevo protocolo.

3.2.2 Fase de implementación del protocolo IPv6

Luego de llevar a cabo la fase de planeación de la transición, se debe poner en marcha aquello que fue establecido, en donde también, se llevarán a cabo las siguientes actividades, en concordancia con lo establecido en:

- Habilitación del direccionamiento IPv6 para cada componente de hardware y software, según lo establecido de la fase anterior, tomando en cuenta, principalmente el inventario de TI.
- Ejecución de la configuración de las pruebas piloto de IPv6, generando pruebas a los segmentos de red con un número espacial de usuarios que aprovechen la homogeneidad de la red, implementando servicios de filtrado, para evitar traumatismos en el funcionamiento normal de la red.
- Preparación de una zona controlada para realizar las pruebas de funcionalidad del protocolo IPv6, teniendo especial cuidado, en aislar o crear un segmento de red, para permitir aceptar cambios y activaciones necesarias para confirmar la funcionalidad del protocolo IPv6, sin que afecte el ambiente de producción de dichos usuarios.
- Implantación del modelo de transición de IPv6 en la red de la empresa, en donde se debe permitir, en caso de ser necesaria, la coexistencia con los protocolos IPv4 e IPv6.

3.2.3 Fase de pruebas de funcionalidad de IPv6

Como culminación del proceso de transición, es necesario que se realicen pruebas de funcionalidad sobre el protocolo de IPv6, con el fin de validar la implementación del mismo y su correcto desempeño en tema de aplicaciones, servicios y demás sistemas que se ven afectadas por dicho cambio. Para tal fin, deben adelantarse las siguientes actividades, en concordancia a:

- La realización de pruebas y monitoreo de la funcionalidad del protocolo IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad, generando tráfico de IPv6 desde la entidad hacia el internet y viceversa.
- La realización del afinamiento de las configuraciones de hardware, software y servicios de la entidad, tomando como referencia el informe de configuraciones del protocolo IPv6, de la fase pasada.

3.3 Cronograma de Actividades

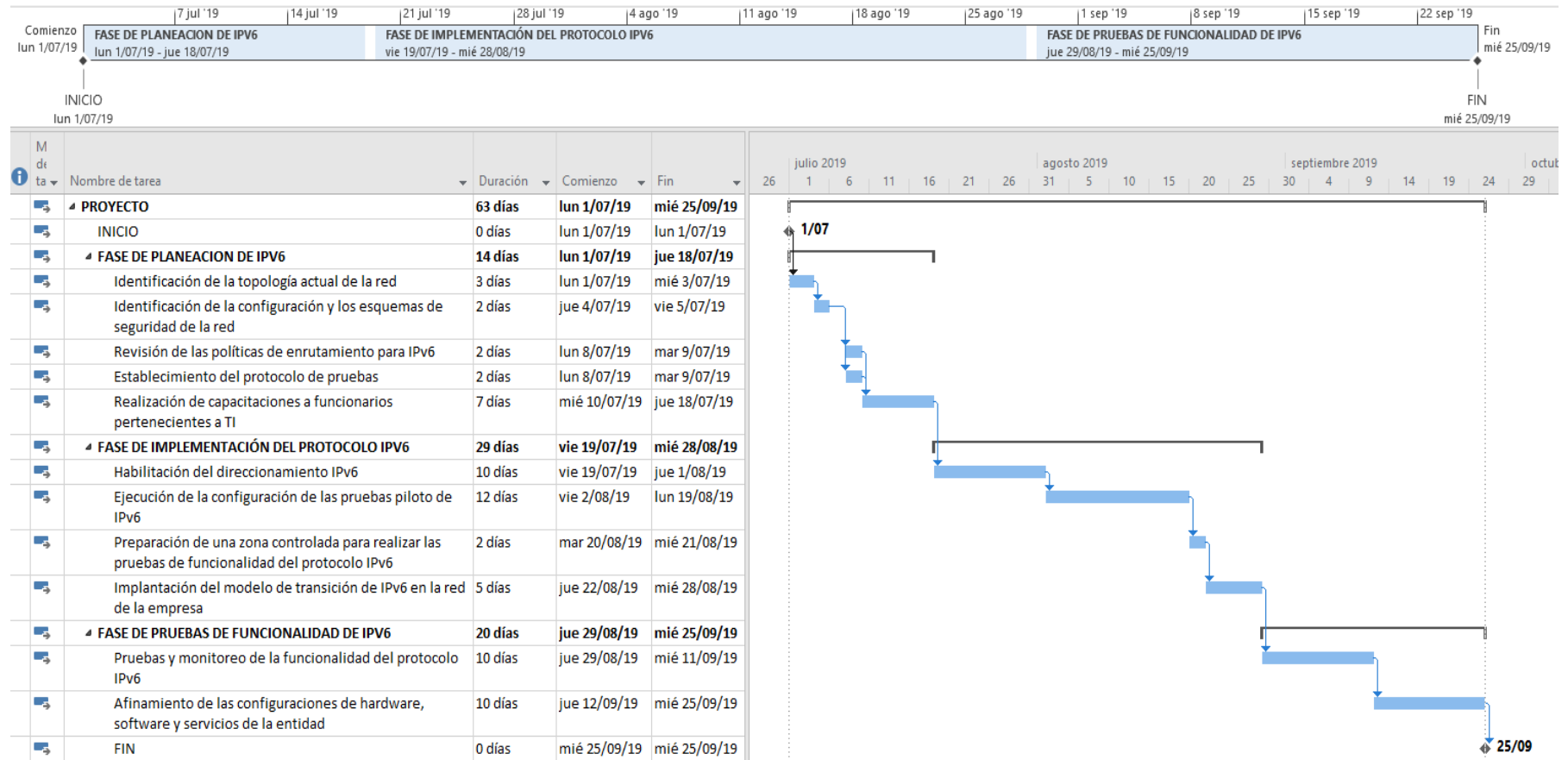


Figura 9: Diagrama de Gantt

Fuente: Elaboración propia

3.4 Aplicando Dual Stack

Como primer método utilizaremos dual stack sobre la red utilizando el host (PC0), host (PC1) y lo que se requiere es que se conecte hacia el servidor principal en el cual se aloja el controlador de dominio y el sistema contable de la empresa

A continuación, veremos cómo configurar el mecanismo de dual Stack (doble pila).

Topología utilizada

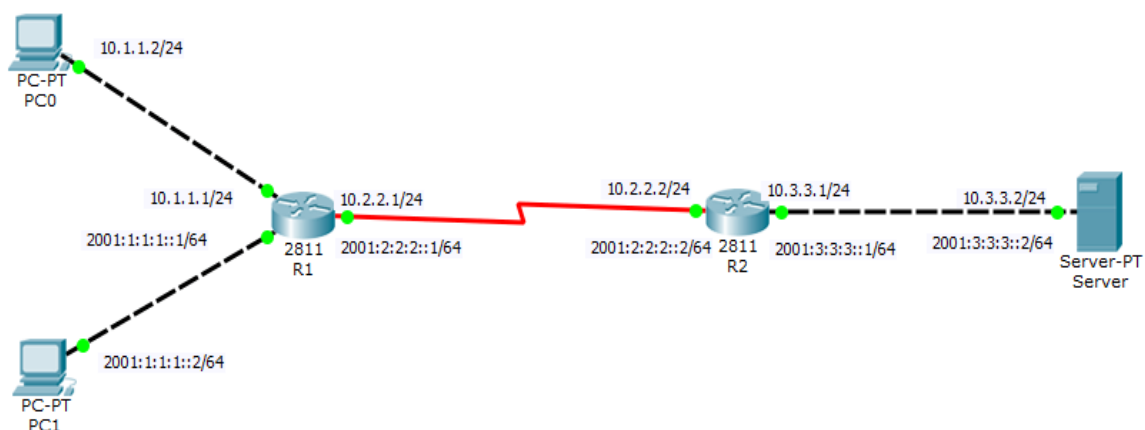


Figura 10: Topología A Utilizar Con Doble Pila

Fuente: Elaboración propia

Configuración en el router R1

```
Router1 # configure terminal
Router1 (config) #interface fastEthernet 0/0
Router1 (config-if) #ip address 10.1.1.1 255.255.255.0
Router1 (config-if) #no shutdown
Router1 (config-if) # interface fastEthernet 0/1
Router1 (config-if) # ipv6 address 2001: 1: 1: 1 :: 1/64
Router1 (config-if) #no shutdown
Router1 (config-if) # interface Serial1 / 0
Router1 (config-if) #ip address 10.2.2.1 255.255.255.0
Router1 (config-if) # ipv6 address 2001: 2: 2: 2 :: 1/64
Router1 (config-if) #no shutdown
Router1 (config-if) #exit
```

Establecer las rutas entre IPv4 e IPv6

```
Router1 (config) # ipv6 unicast-routing
Router1 (config) #ip route 0.0.0.0 0.0.0.0 10.2.2.2
Router1 (config) #ip route :: / 0 2001: 2: 2: 2 :: 2
```

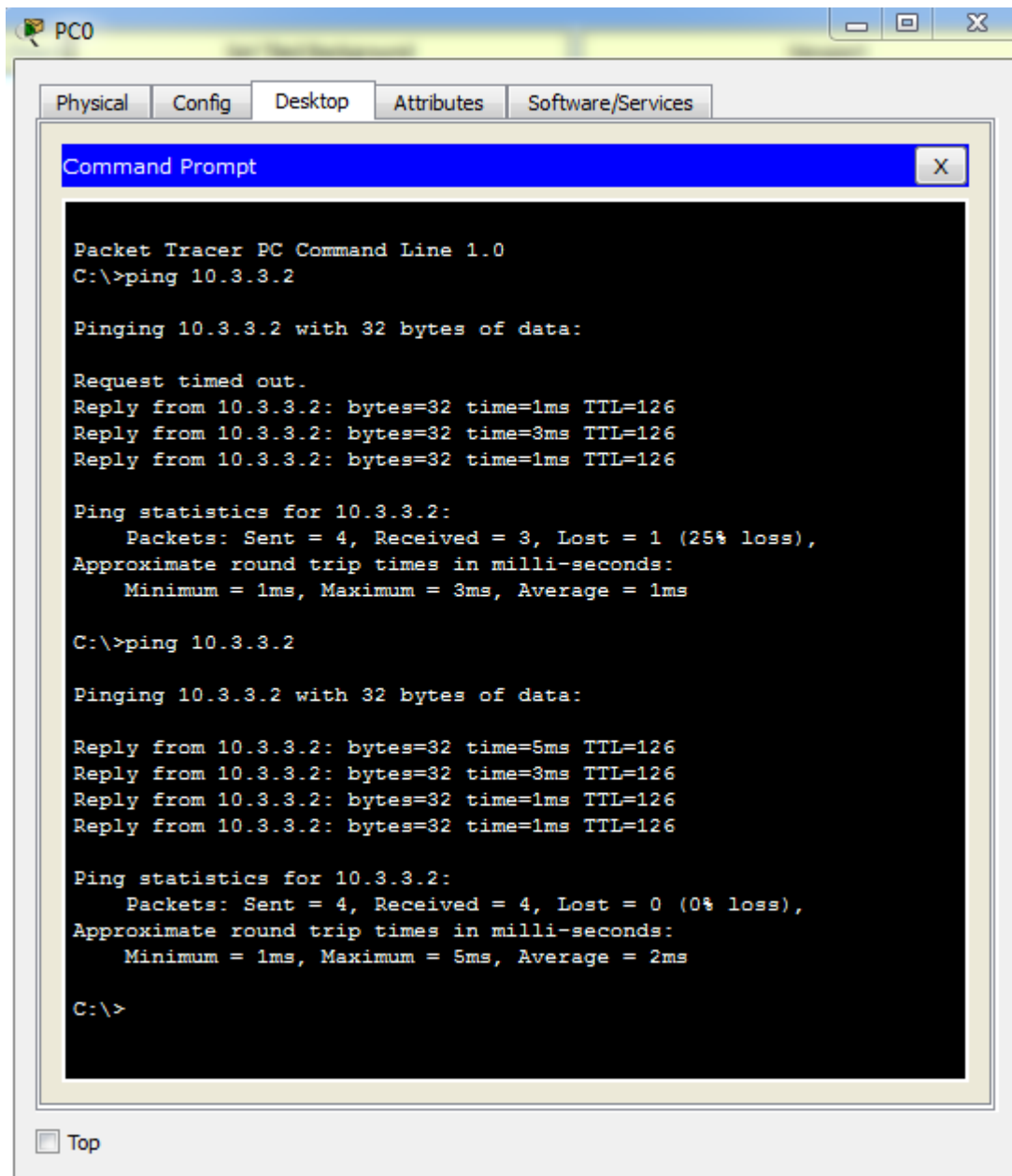
Configuración en el router R2

```
Router2 # configure terminal
Router2 (config) # interface Serial1 / 0
Router2 (config-if) #ip address 10.2.2.2 255.255.255.0
Router2 (config-if) # ipv6 address 2001: 2: 2: 2 :: 2 / 64
Router2 (config-if) #no shutdown
Router1 (config-if) # interface fastEthernet 0/0
Router1 (config-if) #ip address 10.3.3.1 255.255.255.0
Router1 (config-if) # ipv6 address 2001: 3 : 3: 3 :: 1/64
Router1 (config-if) #no shutdown
Router2 (config-if) #exit
```

Establece las rutas entre IPv4 e IPv6

```
Router2 (config) # ipv6 unicast-routing
Router2 (config) #ip route 0.0.0.0 0.0.0.0 10.2.2.1
Router2 (config) # ipv6 route :: / 0 2001: 2: 2: 2 :: 1
```

Pruebas de conectividad



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.3.3.2

Pinging 10.3.3.2 with 32 bytes of data:

Request timed out.
Reply from 10.3.3.2: bytes=32 time=1ms TTL=126
Reply from 10.3.3.2: bytes=32 time=3ms TTL=126
Reply from 10.3.3.2: bytes=32 time=1ms TTL=126

Ping statistics for 10.3.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>ping 10.3.3.2

Pinging 10.3.3.2 with 32 bytes of data:

Reply from 10.3.3.2: bytes=32 time=5ms TTL=126
Reply from 10.3.3.2: bytes=32 time=3ms TTL=126
Reply from 10.3.3.2: bytes=32 time=1ms TTL=126
Reply from 10.3.3.2: bytes=32 time=1ms TTL=126

Ping statistics for 10.3.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

Figura 11: Prueba De Ping Desde PC0 Hacia El Servidor Usando Ipv4

Fuente: Elaboración propia

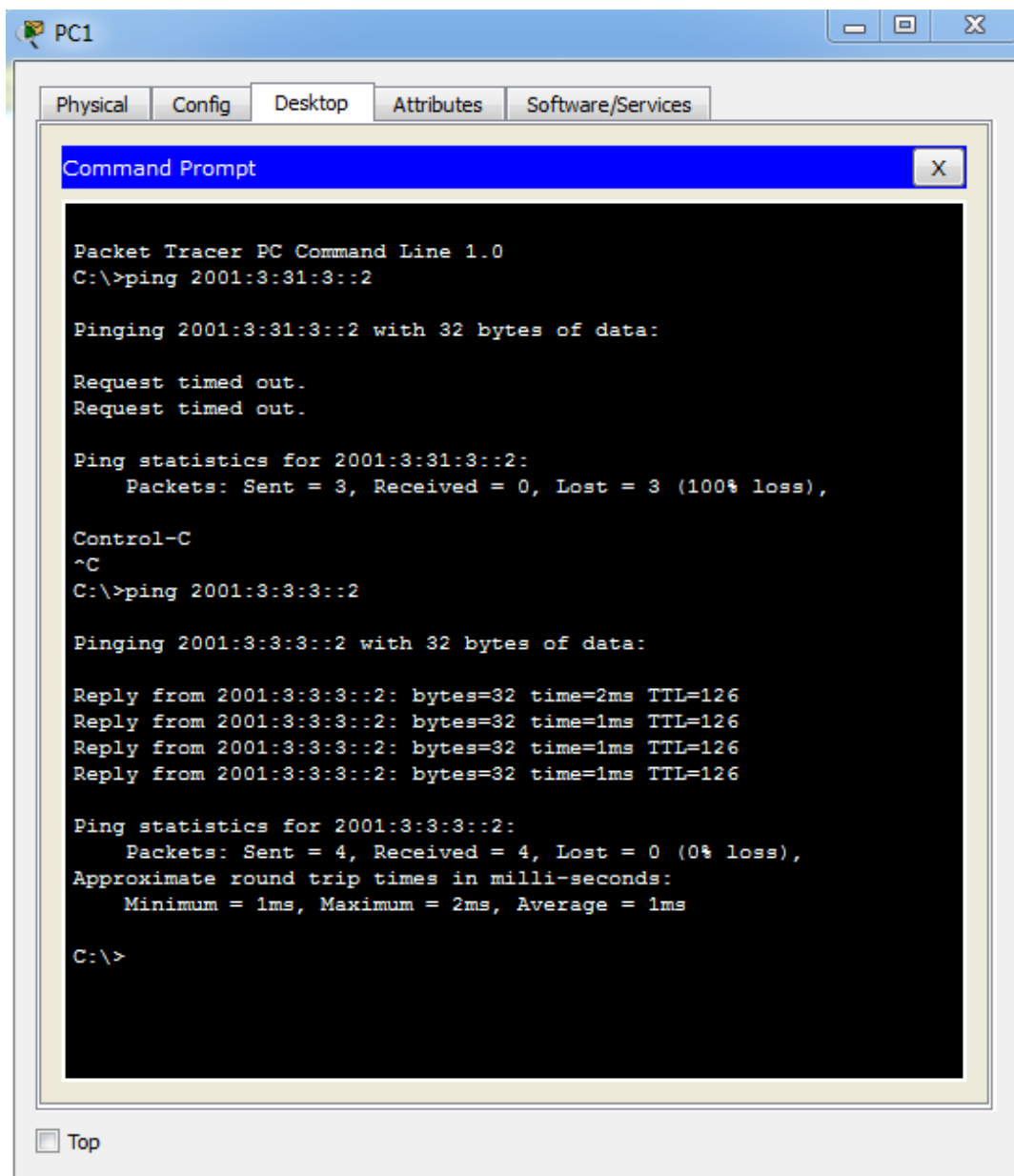


Figura 12: Prueba De Ping Desde PC1 Hacia El Servidor Usando Ipv6

Fuente: Elaboración propia

3.5 Aplicando Túneles

Como segundo método utilizaremos 6over4 sobre la misma red utilizando el mismo host (PC01) y lo que se requiere es que se conecte hacia el servidor principal en el cual se aloja el controlador de dominio y el sistema contable de la empresa

A continuación, veremos cómo configurar el mecanismo de tunelización 6over4.

Topología utilizada

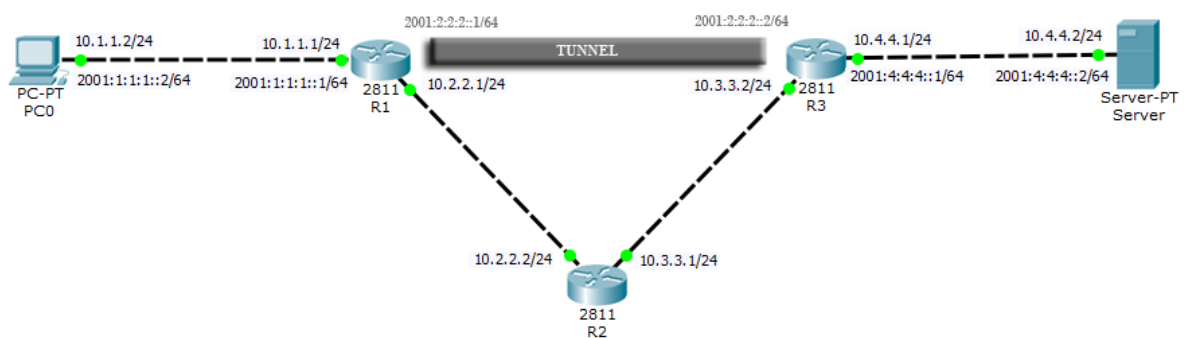


Figura 13: Topología a utilizar con tunelización 6over4

Fuente: Elaboración propia

La topología que se muestra no es una pila dual ya que el Router R2 es solo IPv4 y no es compatible con IPv6.

Configuración del router R1

```
Router1 # configure terminal
Router1 (config) #interface fastEthernet 0/0
Router1 (config-if) #ip address 10.1.1.1 255.255.255.0
Router1 (config-if) # ipv6 address 2001: 1: 1: 1 :: 1/64
Router1 (config-if) #no shutdown
Router1 (config-if) #interface fastEthernet 0/1
Router1 (config-if) #ip address 10.2.2.1 255.255.255.0
Router1 (config-if) #no shutdown
Router1 (config-if) ) #exit
```

Establecer ruta IPv4

```
Router1 (config) #ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Activar enrutamiento IPv6

```
Router1 (config) # ipv6 unicast-routing
```

Configurar Tunnel

```
Router1 (config) #interface tunnel 0  
Router1 (config-if) #tunnel mode ipv6ip  
Router1 (config-if) # ipv6 address 2001: 2: 2: 2 :: 1/64  
Router1 (config-if) #tunnel source fastEthernet 0/1  
Router1 (config-if) #tunnel destination 10.3.3.2  
Router1 (config-if) #exit
```

Establecer rutas IPv6 sobre el túnel

```
Router1 (config) # ipv6 route :: / 0 2001 : 2: 2: 2 :: 2
```

Configuración del router R2

```
Router1 # configure terminal  
Router1 (config) #interface fastEthernet 0/0  
Router1 (config-if) #ip address 10.2.2.2 255.255.255.0  
Router1 (config-if) #no shutdown  
Router1 (config-if) #interface fastEthernet 0/1  
Router1 (config-if) #ip address 10.3.3.1 255.255.255.0  
Router1 (config-if) #no shutdown  
Router1 (config-if) #exit
```

Establecer las rutas IPv4

```
Router1 (config) #ip route 10.1.1.0 255.255.255.0 10.2. 2.1  
Router1 (config) #ip route 10.4.4.0 255.255.255.0 10.3.3.2
```

Configuración del router R3

```
Router1 # configure terminal  
Router1 (config) #interface fastEthernet 0/0  
Router1 (config-if) #ip address 10.3.3.2 255.255.255.0  
Router1 (config-if) #no shutdown  
Router1 (config-if) #interface fastEthernet 0/1  
Dirección Router1 (config-if) #ip 10.4.4.1 255.255.255.0  
Router1 (config-if) #no shutdown  
Router1 (config-if) #exit
```

Establecer Rutas IPv4

```
Router1 (config) #ip route 0.0.0.0 0.0.0.0 10.3. 3.1
```

Habilitar enrutamiento IPv6

```
Router1 (config) # ipv6 unicast-routing
```

Configurar Tunnel

```
Router1 (config) #interface tunnel 0  
Router1 (config-if) #tunnel mode ipv6ip  
Router1 (config-if) # ipv6 address 2001: 2: 2: 2 : : 2/64  
Router1 (config-if) #tunnel source fastEthernet 0/0
```

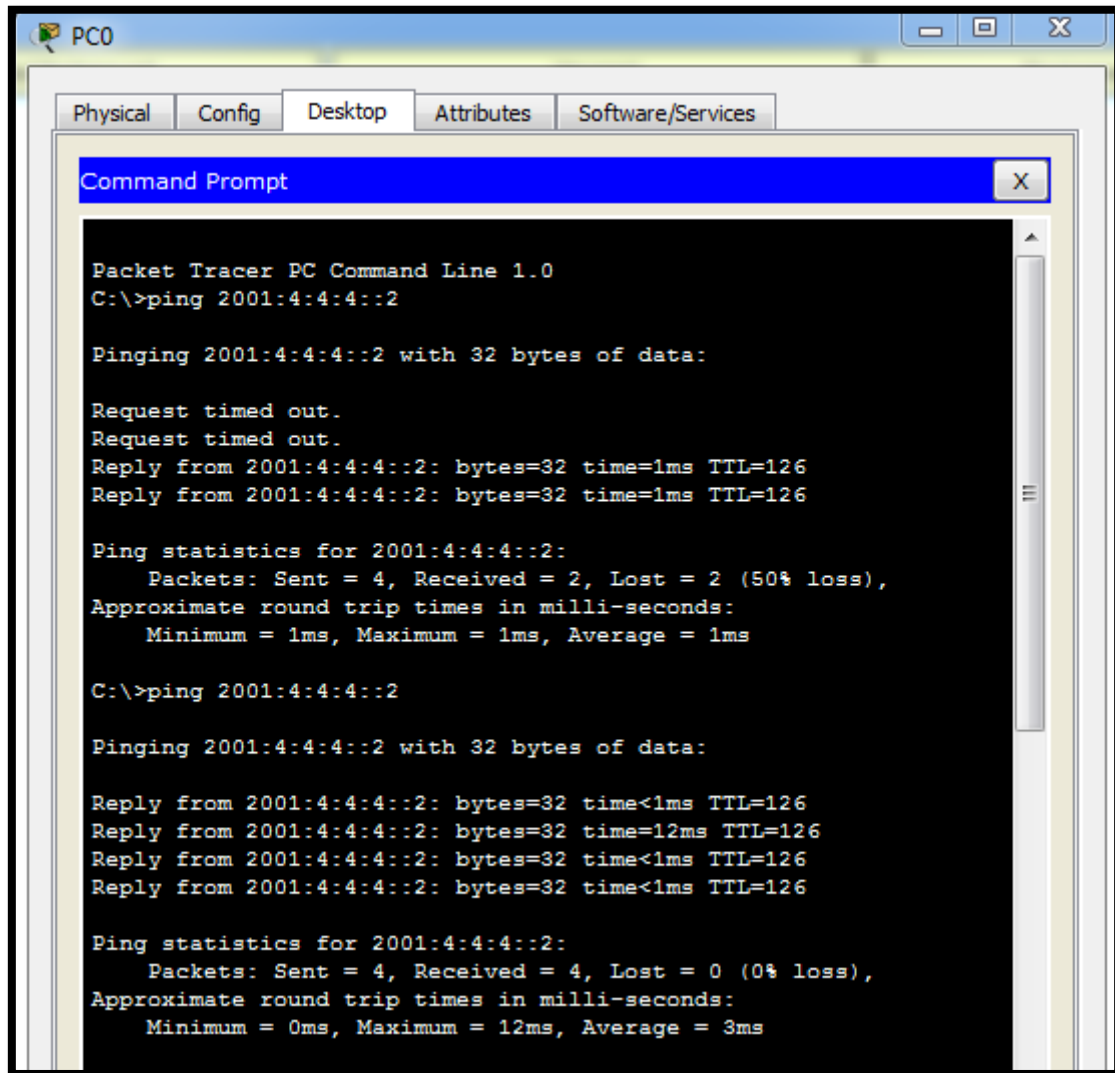
Router1 (config-if) #tunnel destination 10.2.2.1

Router1 (config-if) #exit

Establecer las rutas IPv4

Router1 (config) # ipv6 route :: / 0 2001: 2: 2: 2 :: 1

Prueba de conectividad



```
PC0
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:4:4:4::2

Pinging 2001:4:4:4::2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=126
Reply from 2001:4:4:4::2: bytes=32 time=1ms TTL=126

Ping statistics for 2001:4:4:4::2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 2001:4:4:4::2

Pinging 2001:4:4:4::2 with 32 bytes of data:

Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=126
Reply from 2001:4:4:4::2: bytes=32 time=12ms TTL=126
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=126
Reply from 2001:4:4:4::2: bytes=32 time<1ms TTL=126

Ping statistics for 2001:4:4:4::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

Figura 14: Prueba de ping desde PC0 hacia el servidor usando IPv6

Fuente: Elaboración propia

Como se observa con la tunelización se valida la correcta conectividad hacia el servidor mediante el protocolo IPv6, pero observemos lo siguiente, al iniciar este Ping desde la PC01 hacia el servidor, se tuvo un delay (demora) de conexión de aproximadamente 2 segundos, no afectó en mucho a la conectividad, pero a comparación de doble pila el cual fue el primer utilizado, este último solo tuvo una demora de 1 segundo.

Para ambos métodos se verifica conectividad de host a servidor, por tanto, se asegura que al utilizar doble pila o tunelización, el resultado será el indicado y la conexión que se requiere hacia el destino.

3.6 Acerca de Traducción

El primer método que se introdujo para proporcionar servicios de traducción IPv6 fue la Traducción de direcciones de red - Traducción de protocolos (NAT-PT). NAT-PT simplemente traduce paquetes IPv6 en paquetes IPv4. Este mecanismo ha sido desaprobado por el IETF, debido a su estrecho acoplamiento con el sistema de nombres de dominio (DNS) y sus limitaciones generales en la traducción debido a sus formatos de encabezado complicados en el protocolo IPv4. Las técnicas de traducción estaban destinadas a ser utilizadas como último recurso. Las técnicas de doble pila y túnel son preferibles a las técnicas de traducción.

3.7 Analizando los métodos

Como se ha podido observar, se han visto los métodos (doble pila y túneles), probados con la misma red interna y en diferentes situaciones, esto nos conlleva a poder identificar cuál de los métodos es el más indicado.

A continuación, se presenta un cuadro el cual me sirve de apoyo para validar algunos datos y hacer una comparación de los métodos ya vistos.

Tabla 4: **Cuadro comparativo de los métodos de migración**

	Dual Stack	Túneles	Traducciones
Tiempo	Se realizó la configuración para ambos casos y se validó conectividad hacia el servidor principal, sin ningún problema.	Se realizó la configuración para ambos casos y se validó conectividad hacia el servidor principal, sin ningún problema.	-
Alcance	A toda la red	A toda la red	-
Costo	Verificar el costo de implementación en el apartado 3.6	Verificar el costo de implementación en el apartado 3.6	-
Operación	Se realizó la configuración, tanto en los equipos router internos de la empresa y en los host que se encontraban según topologías.	Se realizó la configuración, tanto en los equipos router internos de la empresa y en los host que se encontraban según topologías.	-
Herramientas usadas	Conocimientos básicos de configuración de equipos router a nivel de interfaz de líneas de comandos.	Comandos intermedios de configuración de equipos router a nivel de interfaz de líneas de comandos.	-
Aceptación	Es aceptable y fácil de realizar.	Es aceptable pero con un nivel más alto de realización a nivel de configuraciones.	-

Fuente: Elaboración propia

3.8 Costos de implementación

Dentro del proceso de migración uno de los temas fundamentales son los costos, debido a que en la inversión que se realizará se requiere la obtención de bienes y servicios que van a formar parte de la infraestructura actual o de una nueva.

En el presente análisis consiste en evaluar temas como:

- Software
- Hardware
- Capacitaciones

A nivel de Software, prácticamente todos los programas soportan IPv6 y si por ahí existe alguno que no es compatible, habrá que buscarle la actualización más reciente de internet e instalarlo. En esta tabla mencionamos el software que utiliza cada host (PC, servidor, etc.), de igual manera tener en cuenta de que este software esta licenciado y no es necesario la activación de alguna adicional.

Tabla 5: **Software que soporta IPv6**

ITEM	SOPORTA IPV6?	COSTO (\$)
SISTEMAS OPERATIVOS		
Windows 7/10	SI	0
Windows Server 2016	SI	0
Apple MAC OS	SI	0
NAVEGADORES DE INTERNET		
Google Chrome	SI	0
Mozilla Firefox	SI	0
Internet Explorer	SI	0
	TOTAL	0

Fuente: Elaboración propia

A nivel de Hardware, se ha verificado que contamos con una amplia variedad de equipos que soportan IPv6, pero agrego unos adicionales por si estos equipos tienden a averiarse.

Tabla 6: **Hardware que soporta IPv6**

Cantidad	Equipo	Marca	Posee la empresa	Soporta IPv6?	Costo por c/u (\$)	TOTAL (\$)
	Cableado	Categ. 6	SI	SI	0	0
	Switch	Cisco	SI	SI	0	0
1	Router	Cisco	SI	SI	2000	2000
					TOTAL (\$)	2000

Fuente: Elaboración propia

Finalmente, a nivel de capacitaciones, conlleva agregar las pruebas de funcionamiento, capacitaciones al personal de TI y a usuarios finales

Tabla 7: **Costos de capacitaciones**

DESCRIPCION	CANTIDAD (Horas)	COSTO POR HORA (\$)	TOTAL(\$)
Pruebas de funcionamiento	100	50	5000
Capitación al personal de TI	48	50	2400
Capacitación a usuarios	24	30	720
TOTAL (\$)			8120

Fuente: Elaboración propia

Muy aparte de los costos mencionados anteriormente, es importante resaltar y tomar en cuenta ciertos imprevistos que se puedan suscitar como, por ejemplo, un especialista de TI externo a nosotros para un asesoramiento en algunas

configuraciones y temas complejos sobre IPv6, además los costos de hardware y capacitaciones son precios aproximados.

Resumiendo, los costos tendríamos lo siguiente:

Tabla 8: **Presupuesto final**

ITEM	COSTO
Costos de Software	0
Costos de Hardware	2000
Costos de capacitación	8120
Presupuesto de contingencia	5000
TOTAL (\$)	15120

Fuente: Elaboración propia

Teniendo en cuenta este último cuadro, podemos mencionar que la implementación tendría un costo 15120 \$, este monto puede variar depende de las circunstancias, aunque el agregado del presupuesto de contingencia nos ayudara si es que por algún motivo necesitemos algo adicional para la migración.

CONCLUSIONES

- Ya que hay muchas aplicaciones aún funcionando con IPv4, no se puede reemplazar con IPv6 de manera inmediata, sino que todo es un proceso que toma su tiempo, pero para ello deben coexistir hasta que poco a poco IPv4 vaya desligándose y solo quede activo IPv6.
- Se llegaron a ver los métodos de transición y se validó la correcta conectividad hacia los servidores principales, la doble pila (dual Stack), túneles, la doble pila como se vio es un proceso ligero y suave para la transición hacia IPv6; el mecanismo llamado túneles la cual también es una buena opción que debería ser tomada en cuenta por los ISP (proveedores de servicios de internet) para brindar la conectividad entre redes y garantizar la integridad de la información.
- No se llegó a resolver el último método de transición (traducción) ya que ha sido desaprobado por el IETF, debido a su estrecho acoplamiento con el Sistema de nombres de dominio (DNS), sus limitaciones generales y sus formatos de encabezado complicados en el protocolo que IPv4.
- También concluimos que el método de Dual Stack o doble pila es la más rápida y eficiente con respecto a túneles, básicamente por la poca configuración y uso del tiempo que se estima que será necesario para hacer la transición al protocolo IPv6.
- Finalmente se debe indicar que el protocolo IPv6 no es del todo desconocido, ya que ahora muchos fabricantes de dispositivos se están preocupando por agregar IPv6 a sus equipos y otros fabricantes actualizan los firmwares para así lograr tener IPv6 en sus productos.

RECOMENDACIONES

- Se recomienda tener ya preestablecido dicho protocolo IPv6 en los equipos internos, para así evitar atrasos de instalación, ya que en un principio ambos protocolos seguirán juntos por un lapso de tiempo llamado también coexistencia, pero esto no afectará a los equipos ni a las aplicaciones internas, sino será una adaptación hasta que IPv6 pueda ya adaptarse a los dispositivos que se configure.
- Para llegar a una pronta adopción de IPv6 en la empresa BP SUPPORT, se requiere el compromiso y cooperación de todos los involucrados para hacer posible lo planificado y así evitar retrasos, ya que hacer la configuración respectiva en todos los equipos tomaría un tiempo prudente y luego hacer el traspaso hacia el protocolo nuevo.
- Impulsar la difusión de la investigación y formación sobre IPv6 en las pequeñas empresas, para fortalecer la cultura del aprovechamiento racional de esta nueva tecnología en las diferentes instancias para cooperar con el engrandecimiento de la misma en varios sectores económicos.
- El establecimiento de este nuevo protocolo es una necesidad inmediata puesto que la mayoría de las aplicaciones y dispositivos que están siendo desarrollados hacen uso de las ventajas que éste ofrece calidad y clase de servicio.

BIBLIOGRAFIA

- 6sos.org. (2004). El protocolo IPv6. Obtenido de www.6sos.org:
http://www.6sos.org/que_es_ipv6.php
- Americas, U. d. (s.f.). Mecanismos de Transición a IPv6. México.
- Architecture and Infrastructure Committee, F. C. (2009). Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government” (the “Roadmap”), Version 1.0. Obtenido de https://www.itu.int/dms_pub/itu-t/oth/3B/02/T3B020000010001PDFE.pdf
- Architecture and Infrastructure Committee, F. C. (2012). Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government”, Version 2.0. Obtenido de <http://1.usa.gov/1yz5i3x>
- Baltazar, M. A. (2017). MODELO DE REFERENCIA DE TRANSICION DE IPv4 A IPv6 PARA EL SECTOR GOBIERNO DE PERU. Lima.
- Benjamin Ramos Alvarez, A. R. (2004). Avances de la criptología y seguridad de la información. . Madrid: Ediciones Diaz de Santos S.A.
- Bernardini, C. (2005). Windows Scripting Host. Barcelona: ENI.
- Budget., O. o. (2005). “Transition Planning for Internet Protocol Version 6 (IPv6)” (OMB Memorandum M-05-22). Obtenido de <http://1.usa.gov/1D4V4Qt>.
- Calderón, M. (2012). Estudio socio-economico del impacto de adopción de IPv6 en Colombia. Bogotá.
- Cedia. (s.f.). www.cedia.edu.ec. Obtenido de www.cedia.edu.ec/es/sobre-nosotros
- definicionabc.com. (15 de Agosto de 2015). www.definicionabc.com. Obtenido de <http://www.definicionabc.com/tecnologia/internet.php>
- ED.AL, J. D. (2003). Comunicaciones en un entorno industrial. UOC.
- Garometta, O. A. (Enero de 2012). Introducción al direccionamiento IPv6. Obtenido de <https://es.slideshare.net/educatica/introduccion-al-direccionamiento-ipv6>
- Guazmayan, C. (2004). Internet y la investigación científica. . Bogotá: Cooperativa Editorial Magisterio.
- Herrera. (2003). Tecnologías de redes y transmisión de datos. Mexico: Noriega Editores.
- IBM Knowledge Center. (s.f.). Obtenido de Comparación IPv4 e IPv6:
https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_71/rzai2/rzai2compip4ipv6.htm#rzai2compip4ipv6__compaddress
- IBM. (s.f.). www.ibm.com. Obtenido de www.ibm.com/support/knowledgecenter/es/ssw_aix_71/com.ibm.aix.networkcomm/tcpip_ipv6_tunnel.htm
- Internet2. (2015). About us. Obtenido de <http://www.internet2.edu/about-us/>
- Iñigo, J. (2009). Estructuras de redes de computadores (primera edición ed.). Barcelona, España: UOC.

- Juncar, J. A. (2001). Internet. Barcelona: Boixereu.
- June Parsons, D. O. (2008). Conceptos de comunicacion: Nuevas perspectivas (decima ed.). México.
- L.M, V. (2012). Del protocolo TCP/IPv4 al TCP/IPv6. Articulo, Universidad Sergio Arboleda, Bogota.
- LACNIC. (2016). Fases de Agotamiento de IPv4. Obtenido de <http://www.lacnic.net/web/lacnic/agotamiento-ipv4>
- LACNIC. (s.f.). IPv6: "mientras más tiempo pase, más recursos tendrán que invertir". Obtenido de <https://www.lacnic.net/2938/1/lacnic/ipv6-mientras-mas-tiempo-pase-mas-recursos-tendran-que-invertir/>
- LACNIC. (s.f.). Mecanismos de transición. Obtenido de <http://portalipv6.lacnic.net/mecanismos-de-transicion>
- Learning, S. E. (2016). Learning, S. E. (2016). Aprende IPv6. Obtenido de <https://www.tutorialspoint.com/es/ipv6/index.htm>
- Martin, J. C. (2010). Infraestructuras Comunes de Telecomunicaciones En Viviendas y Edificios. Editex.
- Mathom, P. (2004). Windows Server 2003 Servicios de red TCP/IP. . United States of America: ENI.
- McLeod, R. (2000). Sistemas de informacion Gerencial (septima edicion ed.). México: Pearson Educacion.
- Mexico, I. (. (s.f.). IPv6mx. Obtenido de <http://www.ipv6.mx/index.php/component/content/frontpage>
- Ministerio de Tecnologia de la Informacion, y. (s.f.). Obtenido de https://mintic.gov.co/gestioni/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf
- MINTIC. (Julio de 2011). SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. . Obtenido de https://www.mintic.gov.co/gestioni/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf
- Montes, E. F. (2005). Seguridad en Ip con el protocolo de seguridad IPsec para IPv6. Trabajo de graduacion. Guatemala.
- Moya, J. M. (2006). Redes y servicios de telecomunicaciones.
- Nap.pe. (s.f.). www.nap.pe. Obtenido de <http://www.nap.pe/nuestros-asociados/>
- neo.lcc.uma.es. (s.f.). Herramientas Web para la enseñanza de protocolos de comunicación. Obtenido de <http://neo.lcc.uma.es/evirtual/cdd/tutorial/Indice.html>
- Paiola, P. (2016). Windows 10 Instalación y configuración. Barcelona: ENI.
- Peruano, D. O. (Agosto de 2017). elperuano.pe. Obtenido de <http://busquedas.elperuano.pe/download/url/decreto-supremo-que-aprueba-la-formulacion-de-un-plan-de-tra-decreto-supremo-n-081-2017-pcm-1552513-1>
- Presidencia, M. d. (2011). www.ipv6.es. Obtenido de <http://www.ipv6.es/es-ES/transicion/Documents/BOE-A-2011-10786.pdf>

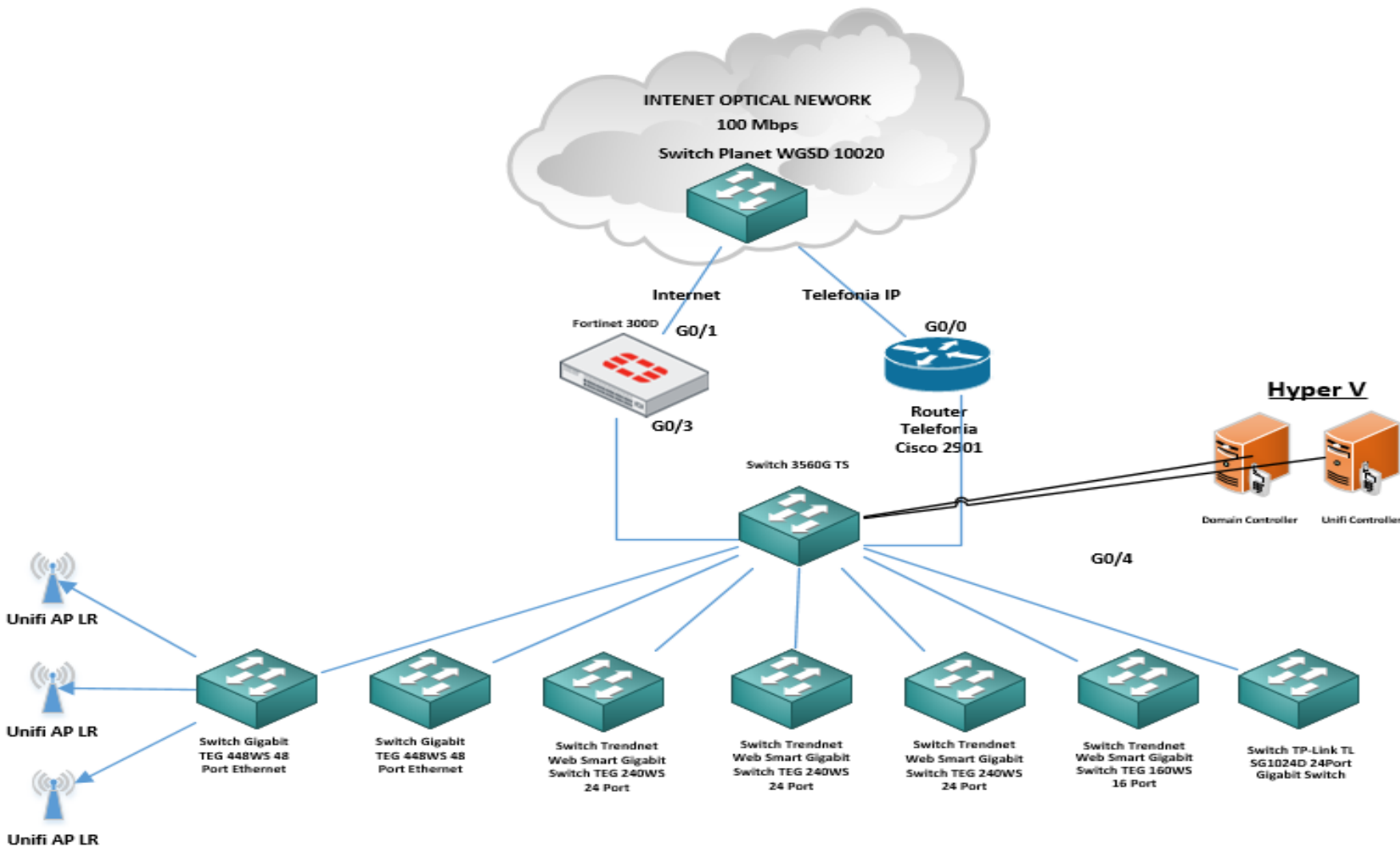
- Públicas., M. d. (2012). administracionelectronica.gob.es. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2012/Marzo/pae_Noticia_2012-03-16_Guia_transicon_a_IPv6_Final.html#.WpqE9SXOWM8
- RedIRIS. (s.f.). www.rediris.es. Obtenido de www.rediris.es/actividades/ipv6day/guia_despliegue_ipv6.html.es
- sites, g. (6 de enero de 2012). Técnica de Migración. Obtenido de <https://sites.google.com/site/123wikiipv6/home/tecnica-de-migracion>
- Tanenbaum, A. &. (2015). Redes de Computadoras (Quinta Edicion ed.). . Mexico: Pearson Educacion.
- Technology., N. I. (2008). A Profile for IPv6 in the U.S.Government – Version 1.0. Obtenido de <http://wwwx.antd.nist.gov/usgv6/docs/usgv6-v1.pdf>
- Technology., N. I. (2009). USGv6: Test Methods:General Description and Validation. . Obtenido de <http://wwwx.antd.nist.gov/usgv6/docs/NIST-SP-500-273.v2.0.pdf>
- Technology., N. I. (2015). USGv6: A Technical Infraestructure to Assist IPv6 Adoption. Obtenido de <http://wwwx.antd.nist.gov/usgv6/index.html>
- Technology., N. I. (2016). Estimating USG IPv6 & DNSSEC External Service Deployment Status. Obtenido de <http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov>.
- Tomasi, W. (2003). Sistemas de Comunicacion Inalambricas. México: Pearson Education.
- Tomasi, W. (2003). Sistemas de comunicaciones electrónicas. Mexico: Pearson.
- Xavier Hesselbach, J. A. (2002). Analisis de redes y sistemas de comunicaciones. . Catalunya: Ediciones virtuales.
- Yair Duran, D. V. (2010). IPv4-IPv6. Universidad Técnica Federico Santa Maria.

ANEXOS

ANEXO A. ROUTER PRINCIPAL 'CORE'



ANEXO B. DIAGRAMA GENERAL DE RED EN LA EMPRESA BP SUPPORT



ANEXO C. RIESGOS INICIALES IDENTIFICADOS Y EVALUADOS A LO LARGO DE LAS DIFERENTES FASES DEL PROYECTO

RIESGOS	IMPACTO	PROBABILIDAD	VALORACION	ACCIONES PARA MITIGAR	FASE
Falta de capacitación del personal técnico.	ALTO	ALTA	ALTO	Refuerzo de conocimientos relacionados al protocolo IPv6 al personal.	Implementación y pruebas
Pérdida de información de los equipos.	ALTO	BAJA	MEDIO	Respaldo de toda la información de la plataforma de TI.	Implementación
Inestabilidad de aplicaciones y SO. Incompatibilidades de SW y HW.	ALTO	MEDIA	ALTO	Revisión y configuración del código de las aplicaciones y SO. Contar con la permanente asistencia técnica del fabricante. Descargar las actualizaciones necesarias.	Implementación y pruebas
Daños físicos en los equipos.	ALTO	BAJA	MEDIO	Mantenimiento y revisión continúa de los equipos (configuraciones). Alcance de los contratos de soporte y mantenimiento.	Implementación
Falta de apoyo Institucional.	ALTO	BAJA	MEDIO	Contar con el apoyo permanente de las personas involucradas en el proyecto.	Todas las fases

Fuente: Elaboración propia

Leyenda:

Impacto: Alto, Medio y Bajo

Probabilidad: Alta, Media y Baja

Cuadro de Valoración:

Alto	M	A	A
Medio	M	M	A
Bajo	B	B	M
	Baja	Media	Alta

Probabilidad