



**FACULTAD DE INGENIERÍA, ARQUITECTURA Y
URBANISMO**

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

**REVISIÓN SISTEMÁTICA DE LOS
MECANISMOS DE TRANSICIÓN PARA LA
MIGRACIÓN DE IPV4- IPV6**

**INFORME DE INVESTIGACIÓN:
PARA OPTAR EL GRADO ACADEMICO DE
BACHILLER EN INGENIERÍA DE SISTEMAS**

Autora:

Chinguel Rodríguez Milagros Maribel

Asesor:

Mg. Tuesta Monteza Víctor Alexci

Línea de Investigación:

Ingeniería, Infraestructura y Tecnología

**Pimentel – Perú
2019**

TABLA DE CONTENIDO

Resumen	3
Abstract	3
I.-Introducción	4
1.1 Antecedentes de estudio.....	5
1.2 Planteamiento del problema de Investigación.	10
1.3 Objetivos.....	10
1.3.1 Objetivo general.	10
1.3.2 Objetivos específicos.....	10
1.4 Marco teórico conceptual.....	11
1.4.1 Protocolo de Internet versión 4(IPv4)	11
1.4.2 Protocolo de Internet versión 6 (IPv6)	16
1.4.3. Mecanismos de transición	20
1.4.4 Etapas de migración	35
II.- Método de Investigación	36
2.1 Plan de investigación	36
2.1.1 Interrogantes de la investigación.....	36
2.1.2 Protocolo de revisión.....	36
2.2 Procedimiento de la investigación	38
2.2.1 Identificar las investigaciones relevantes	38
Resultados	78
Conclusiones.....	83
Bibliografía	83

ÍNDICE DE TABLAS

TABLA I CLASES Y RANGO DE DIRECCIONES IPV4	12
TABLA II MÁSCARAS DE DIRECCIONES IPV4 SEGÚN LA CLASE.....	12
TABLA III CONVERTIR BITS A HEXADECIMAL [32]	20
TABLA IV CONFIGURACIÓN DEL MECANISMO DE TUNELIZACIÓN 6TO4 [35]	25
TABLA V CONFIGURACIÓN R1 [36]	27
TABLA VI CONFIGURACIÓN R2 [36]	27
TABLA VII PING ENTRE ROUTER ISATAP Y CLIENTE [36].....	28
TABLA VIII CONFIGURACIÓN R3 (ISATAP CLIENTE ROUTER) [36]	28
TABLA IX BÚSQUEDA DE BASE DE DATOS Y RESULTADOS	38
Tabla X Sintetizar los datos.....	39
Tabla XI Soluciones basandose en Tunelización	78
Tabla XII Artículos que plantean etapas de migración	79
Tabla XIII Artículos que proponen Tipos de Seguridad	80

Tabla XIV AgrupaciÓn por Tipo de Seguridad	80
Tabla XV Artículos que implementan mecanismos de transición	81
Tabla XVI Agrupación por Tipo de Mecanismo de Transición	82

ÍNDICE DE FIGURAS

Fig. 1 Estructura de la dirección IPv4	11
Fig. 2 Conversión de una dirección binaria a decimal en IPv4 [25]	11
Fig. 3 Detalle de la cabecera IPv6 [30]	17
Fig. 4 Topología del Mecanismo Dual Stack [28].....	21
Fig. 5 Configuración del mecanismo Dual Stack [31]	21
Fig. 6 Topología del Mecanismo Tunnelización [28]	22
Fig. 7 Estructura de las direcciones del mecanismo de tunnelización 6to4 [26].....	23
Fig. 8 Estructura del mecanismo de tunnelización 6to4 [26]	24
Fig. 9 Estructura del Mecanismo de Tunnelización 6to4 con un router relay 6to4 [26]..	24
Fig. 10 Formato de las direcciones del mecanismo de tunnelización ISATAP [26].....	26
Fig. 11 Topología del mecanismo de tunnelización ISATAP [26]	26
Fig. 12 Ejemplo del mecanismo de tunnelización ISATAP [33]	27
<i>Fig. 13 Formato del mecanismo de tunnelización 6RD [34]</i>	<i>29</i>
Fig. 14 Ejemplo de configuración del Mecanismo 6RD [34]	30
Fig. 15 Estructura del Mecanismo de Tunnelización automática 6RD [28]	30
Fig. 16 Estructura del mecanismo Túnel Manual IPv6IP [35].....	31
Fig. 17 Formato del mecanismo Túnel Manual IPv6IP [36, p. 5].....	31
Fig. 18 Estructura del mecanismo de traducción NAT [26].....	32
Fig. 19 Ejemplo del mecanismo de Traducción NAT Dinámico [37].....	33
Fig. 20 Ejemplo del mecanismo de Traducción NAT estático [37]	34
Fig. 21 Método de revisión bibliográfica	36

Resumen

En la actualidad la tecnología ha avanzado rápidamente y por lo tanto a aumentado la cantidad de dispositivos que deben utilizar internet. Esto ha ocasionado un agotamiento de direcciones IPv4. El Grupo de Trabajo de Ingeniería (IETF) ya había previsto este problema de IPv4 por ese motivo creó el protocolo de Internet versión 6 (IPv6) con una capacidad de 340 sextillones de direcciones IP. Pero IPv6 es incompatible con IPv4, debido a esto, crearon los Mecanismos de transición para que ambos protocolos de internet coexistan en una sola red. Esto ayuda a las empresas que quieren migrar a IPv6 sus servicios de forma gradual, ya que es la única forma en que la red no se vea tan afectada al realizar la migración. Los diversos mecanismos han sido evaluados por varios autores para analizarlos y observar su rendimiento, seguridad y posibles casos en los que no podrían abarcar la infraestructura de red. Esto a ocasionado que los mecanismos ya propuestos sean mejorados dando, así como resultado nuevas técnicas de implementación. Los protocolos de Internet tienen un tipo de seguridad que es IPSEC, con la revisión bibliográfica que se hizo se observó que hay algunos autores que deciden solo utilizar IPSEC, otros implementan algún tipo de Firewall, IDS, ACL, SSL y en otros casos modelos híbridos.

Palabras clave: mecanismos de transición, IPv6, IPv4, estrategias de transición, mecanismos de túnel, mecanismos de traducción, Dual Stack

Abstract

At present, technology has advanced rapidly and therefore the number of devices that should be used on the Internet has increased. This has caused an exhaustion of IPv4 addresses. The Engineering Working Group (IETF) had already anticipated this problem of IPv4 for that reason created the Internet Protocol version 6 (IPv6) with a capacity of 340 sextillion IP addresses. But IPv6 is incompatible with IPv4, because of this, they created the transition mechanisms for both internet protocols coexist on a single network. This results in an IPv6. The various mechanisms have been evaluated by several authors to analyze and observe their performance, security and possible cases in which they cannot cover the network infrastructure. This is an opportunity for mechanisms and services to be improved. Internet protocols have a type of security that is IPSEC, with the literature review that showed that there are some authors who decide to only use IPSEC, others implement some type of Firewall, IDS, ACL, SSL and in other cases hybrid models.

Keywords: Transition mechanisms, IPv6, IPv4, Transition strategies, Tunneling mechanisms, Translation mechanisms, Dual Stack

I.-Introducción

Es necesario mencionar que cualquier dispositivo que tenga conexión a internet se le deberá asignar una dirección IP para ingresar a la red. El protocolo de internet que se está utilizando actualmente es la versión 4 que se le conoce como IPv4. Este protocolo contiene 4 mil millones de direcciones IP, sin embargo, estas direcciones son insuficientes para cubrir la gran demanda de conexión a Internet, en la actualidad esto ha generado que IPv4 agote sus direcciones IP [1]. Según [2], IPv4 se encuentra en la última fase de agotamiento (Fase 3) y es por esta razón que se están evaluando estrictamente las solicitudes de los proveedores que desean adquirir más direcciones IP para su uso comercial. Gracias a estas evaluaciones es que se está dosificando adecuadamente la distribución de direcciones IP. Debido a la gran demanda de conexiones, Latin America & Caribbean Network Information (LACNIC) no contará con más direcciones IPv4 y para tener una idea de cuándo será el fin de esta fase de agotamiento. Se realizó una proyección lineal tomando en cuenta las asignaciones que se han hecho a partir de febrero del 2017. Y se concluye que el fin de esta fase será el 27 de enero del 2020 con un factor de error de -0.72.

Al observar que IPv4 se agotaría se creó el protocolo de Internet versión 6 (IPv6) con 128 bits, con una capacidad de 340 sextillones de direcciones IP, capacidad suficiente para poder realizar Internet de las cosas [3].

Según el reporte de [4] desde el año 2008 la implementación del protocolo IPv6 se ha incrementado considerablemente, inició con 0.04% y hasta el 13 de noviembre de 2018 tiene 20.95% de implementación a nivel mundial.

En cuanto a la adopción de IPv6 por países, Bélgica está en el primer puesto ya que fue el primer país en implementar dicho protocolo desde el momento que se creó, por lo que tiene un 53.13 %. En segundo lugar, se encuentra Alemania con 38,48 %, seguido de India con 34.76 %. Sin embargo, en Perú, la adopción es de 15.54% [4].

Google y Microsoft están realizando una gran inversión económica al ir implementando gradualmente IPv6 para que sus servicios no tengan caída en el mercado cuando se agote IPv4 [5].

Gran parte de las organizaciones, su infraestructura de red soporta IPv4. Estas organizaciones deben migrar de IPv4 a IPv6 debido a que en menos de dos años ya se agotará las direcciones IPv4 y si no migran a IPv6, se podría generar pérdidas económicas en la empresa. [6].

Los protocolos de Internet IPv4 e IPv6 no pueden estar en una misma red debido a que su estructura es diferente. Por esta razón el Grupo de Trabajo de Ingeniería de Internet (IETF) creó mecanismos de transición para migrar a IPv6 de forma gradual, sin que los clientes se dieran cuenta que su proveedor de servicio está cambiando de protocolo de red. [7].

1.1 Antecedentes de estudio

Se presenta un enfoque de doble pila. La técnica de tunelización dinámica se utiliza para encapsular un paquete IPv4 en un paquete IPv6 para lograr una transición transparente y escalable. Esta técnica, junto con el enfoque de pila doble, permite que las aplicaciones IPv4 se ejecuten e interactúen con otras aplicaciones IPv4 en entornos de red tanto IPv4 como IPv6 sin ninguna modificación ni recopilación, y sin NAT (traductor de direcciones de red). [8]

IPv6 es una evolución natural de IPv4 e intenta solucionar muchos de los defectos del protocolo anterior. IPv6 está diseñado para mantenerse al día con el rápido crecimiento de Internet. Las especificaciones principales se han estandarizado a través del grupo de trabajo de IPng de IETF, y el grupo de trabajo de NGtrans está estudiando los problemas relacionados con la difícil tarea de realizar una transición sin problemas de IPv4 a IPv6. El documento analiza los beneficios de IPv6 y los obstáculos para su implementación. [9]

Se espera que estos dos protocolos coexistan durante varios años durante el período de transición. Una serie de herramientas de transición de IPv4 a IPv6 están disponibles para atender las diversas necesidades de las diferentes redes. Las dos herramientas de transición más básicas disponibles son el mecanismo de apilado híbrido y la tunelización. Un host híbrido o de doble pila, implementa tanto IPv4 como IPv6, generalmente en una única pila en la que la mayoría del código es compartido por los dos protocolos. La tunelización es la encapsulación del tráfico IPv6 dentro de los paquetes IPv4 para que puedan enviarse a través de una infraestructura IPv4, permitiendo que los hosts y enrutadores de IPv6 se comuniquen sin la necesidad de actualizar la infraestructura de IPv4 que existe entre ellos. [10]

El tamaño y la estructura limitados del espacio de direcciones de Internet de IPv4 han causado dificultades para hacer frente al aumento explosivo en el número de usuarios de Internet. IPv6 es una solución viable para los problemas identificados con IPv4. El Inter funcionamiento eficiente entre IPv4 e IPv6 es muy importante, porque las redes y los servicios de IPv4 existirán durante bastante tiempo. El período de transición será prolongado y se necesitarán equipos de red / terminal que admitan ambas versiones de IP durante el período de transición. Por lo tanto, los problemas de transición de IPv4 a IPv6 requieren especial cuidado y atención. Los tres métodos principales de transición son las pilas duales IPv4 / IPv6 en elementos / terminales de red, túneles y traductores en la red. Se pueden identificar tres fases de transición de IPv4 a IPv6. Estas fases se describen. También se analizan diferentes escenarios de transición desde el punto de vista de la red móvil 2G / 3G. Finalmente, se extraen algunas conclusiones y se dan algunas recomendaciones sobre el uso de los métodos de transición. [11]

IPv6 ofrece ventajas significativas sobre el IPv4 actual, sin embargo, llevará mucho tiempo reemplazar IPv4 por IPv6. Por lo tanto, se espera que estos dos protocolos coexistan durante el período de transición. El Grupo de Trabajo de Transición de Próxima Generación de IETF propone una serie de mecanismos de transición. Sin embargo, la mayoría de ellos proporcionan solo el mecanismo para iniciar sesiones desde hosts dentro de la red IPv6 a aquellos dentro de la red IPv4, pero no admiten la iniciación desde hosts IPv4 a IPv6. En este documento, proponemos el mecanismo de transición de pila dual de IPv4 a IPv6 (4to6 DSTM) que puede funcionar incluso en el caso de que los hosts en la red IPv4 inicien conexiones dentro de los hosts en la red IPv6. [12]

La transición de IPv4 / IPv6 siempre ocurre durante el proceso de implementación de servicios basados en IPv6 a través de Internet IPv4. El Grupo de Trabajo de Transición de Próxima Generación de IETF (NGtrans) ha propuesto muchos mecanismos de transición para permitir la integración perfecta de las instalaciones de IPv6 en las redes actuales. Este trabajo aborda principalmente el rendimiento de los diversos mecanismos de transición de túneles utilizados en diferentes redes. El efecto de estos mecanismos en el rendimiento de las aplicaciones de extremo a extremo se explora utilizando métricas como la latencia de transmisión, el rendimiento, la utilización de la CPU y la pérdida de paquetes. La latencia y el rendimiento medidos del mecanismo 6to4 son mejores que los mecanismos de corredores de túnel y túnel configurados en un 89.38% y 94.83%, 42.47% y 48.76%. Sin embargo, el mecanismo 6to4 debe trabajar mucho más (mayor sobrecarga) para cada paquete enviado, y, por lo tanto, debe ejecutarse a una mayor utilización de la CPU del enrutador de borde. Los paquetes más grandes tenían tasas de pérdida más altas, para los tres mecanismos de tunelización. [13]

IPv6 ha sido diseñado, entre otras cosas, para proporcionar un espacio de direcciones ampliado para satisfacer los futuros requisitos de red. En este artículo, analizamos y discutimos aspectos importantes de los escenarios de implementación de IPv6, y proponemos la arquitectura del sistema que coexiste e integra con las redes IPv4 / MPLS. Investigamos varias estrategias de implementación de IPv6 junto con ejemplos de diseño de red, comparando estas técnicas. Luego se propone el despliegue de IPv6 en entornos de proveedores de servicios. [14]

Aunque IPv6 se ha desarrollado durante más de una década, IPv4 sigue siendo el protocolo de red más comúnmente adoptado. Sin embargo, los cambios significativos en la nueva versión pueden hacer que el procedimiento de transición continúe durante varios años. Actualmente, se proponen tres mecanismos de transición, pila doble, tunelización y traducción para resolver los problemas debido a la coexistencia de IPv6 e IPv4. En muchas ocasiones, podría haber más de un mecanismo

de transición entre las conexiones de red. Con el fin de gestionar eficazmente el entorno coexistente con diversos mecanismos de transición, este documento presenta un enfoque práctico para abordar la gestión de redes coexistentes. En este enfoque, primero determinamos las transiciones subyacentes mediante la recopilación y el análisis de las direcciones IPv6 correspondientes. Una vez que se descubren las transiciones [15]

Este documento se enfoca en los escenarios de implementación de IPv6 a través de MAN de acceso múltiple y de bordes múltiples, asumiendo una infraestructura basada en DSL. Se proporciona una perspectiva completa de extremo a extremo, incluido el impacto de dicha implementación en los diferentes elementos de MAN. El documento reúne y analiza el impacto de las soluciones y características actuales de IPv6, aplicándolas a un conjunto relevante de modelos de conectividad mayoristas, considerando los escenarios de coexistencia nativos de IPv6 e IPv4 / IPv6 [16]

Hasta hoy, se han realizado muchos estudios para el mecanismo de transición de IPv6, pero parece tener muchas dificultades para expandir la red de IPv6 debido a la falta del servicio de IPv6 y los problemas de interfuncionamiento no resueltos con la red de IPv4. Este documento propone un nuevo mecanismo de transición de IPv6 basado en un túnel de extremo a extremo que es un método fácil de expandir para implementar los servicios de IPv6. [17]

Pasar de la versión cuatro del protocolo de Internet (IPv4) a la versión seis del protocolo de Internet (IPv6) no es sencillo porque IPv4 y IPv6 son protocolos incompatibles. Para permitir una integración sin problemas entre IPv4 e IPv6, el Grupo de Trabajo de Transición de IPng IETF (NGTrans) ha propuesto varios mecanismos de transición. Uno de ellos es el mecanismo de transición de pila dual (DSTM). Este documento revisa la implementación de DSTM sobre nuestro banco de pruebas de IPv6 (6iNet) en la Universidad Utara Malaysia (UUM). Este documento también describe nuestra experiencia en la configuración de 6iNet. 6iNet es el primer banco de pruebas de IPv6 en UUM y se ha convertido en una plataforma para la investigación de IPv6 en UUM [18]

El Departamento de Defensa (DoD) de los EE. UU. Planea agregar la capacidad del protocolo de Internet (IP) versión 6 (IPv6) a todas las redes IP del DoD para el año 2008 y luego comenzar la eliminación de la versión 4 (IPv4). Para facilitar esta migración, se han desarrollado diversos mecanismos de transición para abordar la interoperabilidad de las redes y sistemas IPv4 e IPv6. A medida que la transición llegue al punto en el que se implementan ampliamente las aplicaciones de IPv6, y la red es dominante en IPv6, se requerirá la traducción entre IPv4 e IPv6 para la interoperabilidad continua de los dispositivos heredados de IPv4. Actualmente se está probando

y evaluando un prototipo experimental de un dispositivo de traducción proxy IPv4-IPv6 simple y de bajo costo en las Redes de Próxima Generación (S & TCD) de la Dirección de Comunicaciones Espaciales y Terrestres (S & TCD) del Ejército de los EE. UU. CERDEC S & TCD XGN está llevando a cabo una investigación adicional sobre la extensión de los beneficios de servicios avanzados y características como IPv6 móvil (MIPv6) y seguridad para dispositivos heredados de IPv4 a través de la integración de traducción y MIPv6. Este documento describe el trabajo en progreso y también explora la implementación de estas capacidades en redes inalámbricas heredadas y de próxima generación. [19]

Se ofrecen varios mecanismos de transición para permitir la adopción gradual de IPv6 y prolongar el útil tiempo de operación de los sistemas y aplicaciones heredados. Los mecanismos de transición realizan conversiones entre las versiones 4 y 6 del protocolo IP, ofrecen funcionalidad de tunelización y actúan como puntos de conexión entre segmentos de red aislados (en el sentido de versiones de IP). En este documento examinamos los mecanismos de transición de IPv6 (centrados en los mecanismos de tunelización) y sus requisitos de gestión. Específicamente, examinamos en el mecanismo más utilizado, 6to4. Presentamos sus características operativas e identificamos sus principales requerimientos de gestión. Estos requisitos se utilizan luego para definir los objetos correspondientes para una base de datos de información de administración (MIB) de SNMP. Nuestro objetivo es utilizar la metodología SNMP para abordar los problemas más importantes del mecanismo de transición de IPv6 en un entorno de administración de red unificada. Nuestro esfuerzo ha dado como resultado un prototipo de agente SNMP que implementa la mayoría de nuestras sugerencias de objetos de administración. Describimos brevemente los desafíos de implementación que enfrentamos y sus principales características operativas. [20]

El dinámico mundo empresarial de hoy está dominado por muchas fusiones y adquisiciones (M&A) que, junto con los beneficios comerciales, pueden tener un impacto en la red IP de las organizaciones combinadas. Las fusiones y adquisiciones pueden llevar a redes IP que son más caras de operar y técnicamente más frágiles debido al agotamiento de direcciones o al espacio de direcciones superpuestas. En algunos casos, se requiere un redireccionamiento costoso y prolongado, y en otros, la superposición de NAT (traducción de direcciones de red), con todas sus implicaciones de gestión, se utiliza para unirlos. Este documento analiza las soluciones de IPv6 que pueden proporcionar acceso completo entre todos los sitios, incluidos los sitios recientemente agregados que se han adquirido a través de M&A. Las soluciones analizadas en este documento brindan acceso inmediato a las aplicaciones que residen en toda la empresa [21]

Se han desarrollado numerosos mecanismos de transición de IPv6 para apoyar la interoperabilidad entre IPv4 e IPv6. Si bien los aspectos de rendimiento de estos mecanismos son requisitos para el despliegue práctico, aún no se han evaluado empíricamente. En este documento presentamos el impacto de los mecanismos de transición de IPv6 en la aplicación del usuario. Nuestros resultados experimentales muestran que, aunque las sobrecargas de rendimiento fueron mínimas, se produjo cierta degradación del rendimiento en paquetes pequeños, fragmentados y de traducción. [22]

Al canalizar paquetes de IPv6 sobre IPv4 UDP, Teredo admite nodos de pila dual IPv4 / IPv6 en redes privadas IPv4 detrás de la traducción de direcciones de red (NAT) para acceder a las redes IPv6. Sin embargo, el protocolo Teredo actual no funciona con NAT simétrica. Esta carta propone SymTeredo, una extensión de Teredo con capacidad para atravesar el NAT simétrico. Nuestra extensión conserva la arquitectura Teredo y ofrece compatibilidad con el protocolo original de Teredo. [23]

La disposición básica para la introducción de servicios de alcance global, como Voz sobre IP (VoIP), en las redes IP heterogéneas de la próxima generación es la accesibilidad ubicua de IPv4, IPv6 y hosts de doble pila. Para una operación de servicio sin interrupciones en diferentes etapas de la evolución de la red, el despliegue de los mecanismos de transición más adecuados para la interconexión de redes IPv4 e IPv6 es de gran importancia. La selección cuidadosa de los mecanismos es necesaria, ya que la configuración diferente de los mecanismos de transición a lo largo de la ruta del servicio puede tener un impacto diferente en el rendimiento del servicio. El trabajo presentado en este documento tiene como objetivo la caracterización del rendimiento de varios escenarios de redes en los que las aplicaciones de VoIP basadas en SIP interactúan con diferentes mecanismos de transición IPv4-IPv6. [24]

Debido al continuo crecimiento masivo de Internet global, las direcciones de red IPv4 disponibles se agotarán en los próximos años. La solución a este problema es el protocolo IPv6 con su vasto espacio de direcciones. Durante el período de transición de IPv4 a IPv6, ambos protocolos coexistirán, lo que hace necesario contar con técnicas de transición para mantener la interoperabilidad. Estas técnicas de transición tienen un impacto inevitable en el rendimiento de la red. Para cuantificar este impacto, configuramos un banco de pruebas para medir las penalizaciones de rendimiento introducidas por cuatro técnicas de transición. En general, las mediciones del rendimiento de transición se pueden llevar a cabo en diferentes capas. La decisión de elegir el protocolo de inicio de sesión (SIP) como protocolo de capa de aplicación se basa en el hecho de que la voz sobre IP puede ser uno de los principales impulsores de IPv6. [25]

El IPv6 es una tecnología inevitable para la red doméstica ubicua debido al creciente número de productos electrónicos de consumo (CE) y las demandas explosivas de los servicios de red doméstica que requieren conectividad de extremo a extremo a través de Internet. Para proporcionar servicios basados en el IPv6 en la red doméstica, se requieren los mecanismos de transición de túnel a domicilio y de IPv4 / 6 debido a la implementación tardía del IPv6 en la red pública. El documento propone una estrategia de implementación y evalúa el rendimiento de la red doméstica IPv6 en el banco de pruebas utilizando el servidor doméstico, que establece conexiones entre los CE e Internet. Además, el documento también propone un nuevo mecanismo de transición de IPv4 / 6 (proxy ARP / NDP para NAT-PT) para respaldar la interoperabilidad entre varias CE basadas en IPv4 / 6 dentro de una red doméstica [26]

1.2 Planteamiento del problema de Investigación.

¿Cuál es el estado del conocimiento respecto a los mecanismos de transición para la migración de IPv4- IPv6?

1.3 Objetivos.

1.3.1 Objetivo general.

Realizar una revisión del material bibliográfico sobre clasificación no destructiva de frutas utilizando visión artificial

1.3.2 Objetivos específicos.

- Elaborar el plan de investigación
- Desarrollar el procedimiento de investigación
- Crear la documentación de la investigación

1.4 Marco teórico conceptual

1.4.1 Protocolo de Internet versión 4 (IPv4)

El protocolo de Internet versión 4 (IPv4) en la actualidad es el más usado ya que tiene una capacidad de aproximadamente 4000 millones de direcciones IP con un tamaño de direcciones de 32 bits. [27]

La estructura de las direcciones IP está compuesta jerárquicamente y se divide en dos partes identificándose en primer lugar la red y posteriormente a la computadora en la red (Ver Fig. 3).

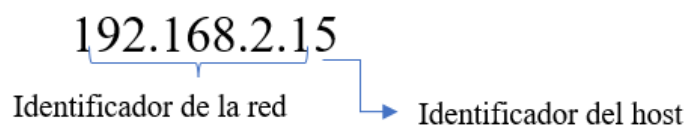


Fig. 1 Estructura de la dirección IPv4

Fuente: Elaboración propia basado en [27]

La parte principal en la dirección IP es el identificador de red ya que de él dependerá el número de identificadores de host que pueda poseer el cliente. [27]

1. Notaciones

La dirección IP consta de 4 bytes, cada byte contiene 8 bits (octetos), para calcular la cantidad de bits se debe multiplicar la cantidad de bytes por bits que saldría un total de 32 bits. Cada octeto se representa por 0 y 1 (código binario). [27] Para convertir una dirección IP al código binario deberá de realizar la siguiente operación:

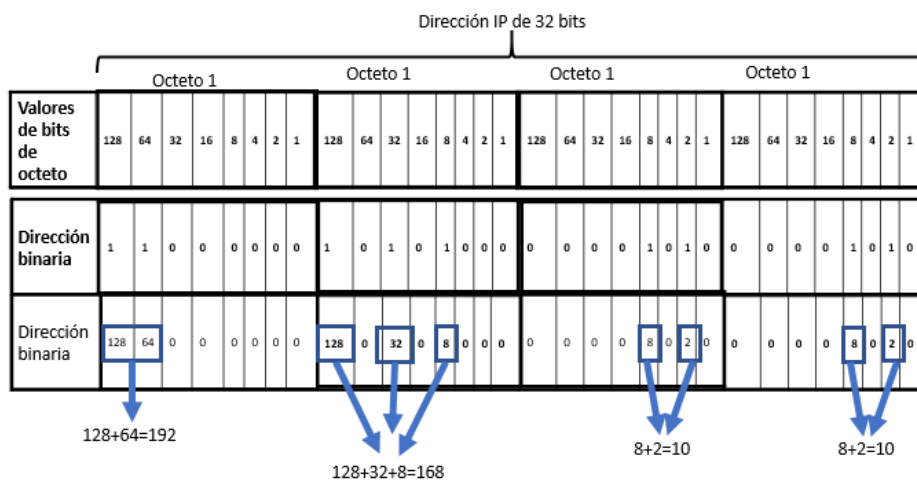


Fig. 2 Conversión de una dirección binaria a decimal en IPv4 [28]

2. Clases de direcciones IP

Estas direcciones IP tienen 5 clases de las cuales a los usuarios solo utilizan desde la clase A hasta la C, ya que la clase D está reservada para realizar multicast y la clase E es solo para uso experimental en casos de estudio. [27]

TABLA I CLASES Y RANGO DE DIRECCIONES IPV4

Clase	Rango	
	Desde	Hasta
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

Fuente: Elaboración propia basada en [27]

3. Máscaras

La máscara dependerá de la clase de dirección de red que se le asignará a la computadora. Esta consta de 32 bits. Los bits que serán para la dirección de red se le asignará uno, y a los que pertenecerá al host cero. [27]

TABLA II MÁSCARAS DE DIRECCIONES IPV4 SEGÚN LA CLASE

Clase	Máscara
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Fuente: Elaboración propia basada en [27]

4. Análisis del formato del datagrama IP

Según [29] los datos que se transmiten por Internet utilizando el protocolo IP viajan en mensajes llamados datagramas IP.

El datagrama IPv4 se divide globalmente en la cabecera y la carga útil (payload). En la cabecera se incluyen los campos de direccionamiento y control, mientras en la carga constan los datos que realmente se envían a la red. Los datagramas IP no añaden una terminación posterior a la carga útil, a diferencia de otros formatos.

Aunque IP es un protocolo relativamente simple, la cabecera del datagrama contiene una buena cantidad de información, como mínimo unos 20 bytes de longitud, y está formado por los siguientes campos.

Versión. 4bits: en este campo se describe la versión de IP que se utilizará para crear el datagrama.

IHL (tamaño de la cabecera). 4 bits. Especifica en palabras de 32 bits la longitud de la cabecera IP. El valor normal de este campo, si no se utilizan opciones, es 5. Su valor máximo puede ser de 15 bits.

TOS (tipo de servicio). 8 bits. Está diseñado para indicar en una serie de parámetros la calidad del servicio. Los últimos cinco bits señalan las características del servicio, mientras los tres primeros, el nivel de urgencia:

000: De rutina.

001: Prioritario

010: Inmediato.

011: Relámpago.

100: Invalidación relámpago.

101: Procesando llamada crítica y de emergencia.

110: Control de trabajo de Internet.

111: Control de red.

LT (Longitud Total). 16 bits. Se especifica la longitud total del datagrama IP en bytes.
Identificador. 16 bits. Solo se utiliza si el datagrama tiene que fragmentarse.

5. Arquitectura TCP/IP

[27] describe que la arquitectura TCP/IP consiste en una compleja arquitectura de red desarrollada en los años 70 por el Departamento de Defensa de Estados Unidos, que incluye varios protocolos agrupados en capas, siendo sin lugar a dudas, la más utilizada en el mundo, ya que es la base de las comunicaciones de Internet.

Su función principal es enlazar y comunicar distintos equipos informáticos en redes de área local (LAN) y área extensa (WAN). TCP determina el control del flujo y los acuse de recibo del intercambio de paquetes, mientras IP identifica el origen y destino según se envían los paquetes por la red.

Los protocolos resultan determinantes en una red, ya que todos los hosts deben hablar el mismo lenguaje, es decir, utilizar o compartir un mismo protocolo. En caso contrario, no podrían comunicarse, resultando inviable la conexión.

[30, p. 21] La arquitectura TCP/IP se estructura en las capas de enlace, red, transporte y la capa de aplicación.

Nivel de enlace

La capa de enlace es el interfaz con el hardware de la red. Este interfaz puede proporcionar o no una entrega fiable y puede ser orientada a paquetes o a flujo de bits. TCP/IP no especifica ningún protocolo en esta capa, pero puede utilizar casi cualquier interfaz de red disponible lo que da una idea de la flexibilidad de la capa superior, la capa IP [30, p. 22].

Nivel de red

El nivel de red es el encargado de encaminar los paquetes a través de la red de manera que lleguen a su destino. El nivel de red es la base de la familia de protocolos TCP/IP, que define el protocolo más importante: IP. [30, p. 22]

Nivel de transporte

[27, p. 13] La capa de transporte se encarga de establecer una conversación entre el origen y el destino sin importar el contenido de los datos. Entre sus funciones se encuentran la corrección de errores, el control de flujo y la confiabilidad de la conexión.

Los principales protocolos de la capa de transporte son TCP y UDP. TCP utiliza acuses de recibo para garantizar al host emisor la recepción de la información enviada. En ocasiones puede no ser necesario el acuse de recibo, ya que disminuye la velocidad de transferencia. En este caso UDP puede resultar el protocolo de transporte más adecuado. No garantiza que la información llegue a su destino, pero existe una probabilidad muy alta de que así sea.

1. TCP:

[27, p. 25] TCP es uno de los protocolos de transporte principales, orientado a conexión, siendo el principal para el envío de datos en Internet. Ofrece una alta confiabilidad sin problemas de flujo y un bajo nivel de errores.

Las aplicaciones que trabajan con UDP toleran pequeñas pérdidas de datos. Generalmente, es usado por aplicaciones de transmisión de vídeo y voz. La radio o televisiones que emiten

en Internet son algunas de las aplicaciones que suelen trabajar con UDP.

Se encarga de mantener un diálogo entre el origen y destino mientras empaqueta información de la capa de aplicación dividida en pequeñas partes, denominadas segmentos.

TCP realiza un seguimiento de la cantidad de segmentos que se envían a un host específico. Si transcurrido un tiempo el host emisor no recibe un acuse de recibo confirmándose la entrega, este vuelve a enviar únicamente los segmentos que se perdieron, no toda la información, hasta confirmarse la entrega al receptor. Los segmentos se enumeran en secuencias y pasan al proceso IP para armarse en paquetes. Para que la comunicación se establezca sin problemas entre dos aplicaciones es necesario que los puertos TCP correspondientes estén abiertos.

Dos ordenadores, normalmente un cliente y un servidor, establecen la comunicación mediante el mecanismo conocido como negociación.

La relación entre IP y TCP resulta importante, ya que IP indica el camino a los paquetes y TCP garantiza un transporte seguro.

Las características más destacadas del protocolo TCP son las siguientes:

- a. Permite colocar en el orden adecuado los datagramas cuando provienen del protocolo IP. Permite que los datos se formen en segmentos de longitud variable.
- b. Monitorea el flujo de datos para evitar la saturación de la red.
- c. Multiplexa datos, es decir, en la misma línea puede circular simultáneamente información que viene de diferentes fuentes.

2. UDP:

[27, p. 83] UDP (User Datagram Protocol) es un protocolo de transporte no orientado a la conexión. No proporciona detección de errores, ya que trabaja sin acuse de recibo, de manera que no hay verificación de la distribución de segmentos. Pero se considera un protocolo de máximo esfuerzo, siendo muy probable que los datagramas lleguen a su destino, aunque es posible que lo hagan de forma desordenada o que se pierdan algunos o todos.

[27, p. 84]UDP transmite segmentos en un encabezado de 8 bytes seguido de la carga útil, compuesto por los siguientes campos:

Puerto de origen: corresponde al número de puerto relacionado con la aplicación del remitente del segmento.

Puerto de destino: número de puerto que corresponde a la aplicación del equipo receptor.

Longitud: indica la longitud total del segmento. Incluye el encabezado de 8 bytes y los datos.

Suma de comprobación: permite controlar la integridad del segmento.

Nivel de aplicación

[30, p. 36] La capa de aplicación es la más alta en la torre de comunicación que representa el modelo TCP/IP. Por ello, es en esta capa donde se implementan las funcionalidades últimas que se pretenden alcanzar, y que requieren una comunicación entre varios nodos. Todos los niveles inferiores del modelo están diseñados para ofrecer a la capa de aplicación unas funciones últimas de comunicación, y esta capa las utilizará para presentar al usuario final.

1.4.2 Protocolo de Internet versión 6 (IPv6)

A. Representación de direcciones de red IPv6

[31] Una dirección de IPv6 está constituida por «128» «bits» representados en formato hexadecimal en ocho bloques de cuatro dígitos separados por el carácter «:». Es decir :

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

Donde cada «x» representa un dígito hexadecimal.

Por ejemplo:

2001:0678:0000:00ab:f500:0000:0000:0001

Existen dos reglas de representación simplificada:

- 1.- Los ceros a la derecha son omisibles. Ala izquierda no.
- 2.Uno o más cuartetos consecutivos formados únicamente por ceros pueden ser sustituidos por «::», pudiéndose aplicar una sola vez.

De este modo, el ejemplo anterior se podría simplificar como:

2001:678:0:ab:f500::1

2001:678::ab:f500:0:0:1

Hay una notación adicional para casos de protocolos que compatibilizan IPv4 e IPv6 y que consiste en definir los últimos «32» «bits» de la dirección IPv6 a partir de la dirección IPv4 en formato decimal.

Es decir: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:d.d.d.d

donde cada «d» representa un dígito en notación decimal.

Por ejemplo: 2001:0678:0:ab:f500::172.20.0.1

Es el caso de auto túneles en los que la dirección IPv6 se deriva a partir de un prefijo y la dirección IPv4 existente. Estas direcciones tienen el requisito de necesitar una máscara de longitud «/96», concepto que se explica en el siguiente punto.

[32, p. 177] El sistema hexadecimal está constituido por 16 símbolos:

{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}

B. Formato del paquete IPv6

[33] Los campos de la cabecera IPv6 son los siguientes:

Versión	Clase de tráfico	Etiqueta de flujo	
Longitud de carga útil		Sig. Cabecera	Límite saltos
Dirección de origen (16 bytes)			
Dirección de destino(16 bytes)			

Fig. 3 Detalle de la cabecera IPv6 [33]

Versión (4-bits): Indica la versión del protocolo IP. En este caso contendrá un 6.

Clase de Tráfico (8 bits). Permite diferenciar clases de tráfico como, por ejemplo, entre tráfico interactivo y tráfico normal. Permite la posibilidad, incluso, de descartar ciertos datagramas en caso de congestión.

Entre las clases de tráfico están las siguientes:

0: Tráfico sin clasificar.

1: Tráfico de ‘relleno’, por ejemplo, noticias en red.

2: Transferencia de datos normal (por ejemplo, tráfico de correo electrónico).

3: Reservado.

4: Transferencias de datos atendidas (por ejemplo, transferencia de ficheros).

5: Reservado.

6: Tráfico interactivo.

7: Tráfico de control de Internet (por ejemplo, mensajes de protocolos de encaminamiento).

Valores de 8 a 15: se pueden utilizar por los mecanismos de control de congestión, si los protocolos de transporte utilizados no realizan dicho control, como es el caso de UDP.

Etiqueta de Flujo. Se trata de una etiqueta que permite diferenciar clases de flujos, permitiendo diferentes tratamientos en función de la etiqueta. De esta manera, se puede señalar el tráfico que necesite tratamiento especial, como es el caso, por ejemplo, del tráfico en tiempo real, que es posible que necesite reserva de ancho de banda.

Longitud de Carga Útil (16 bits). Incluye un entero sin signo que indica la longitud, en bytes, de la carga útil (campo de datos) del datagrama, es decir, del resto del datagrama a partir del último byte de la cabecera. Nótese que las extensiones de cabecera (extension headers) presentes en el datagrama, si existen, se consideran parte de la carga útil, es decir, que estarían incluidas en la longitud indicada en este campo.

Siguiente Cabecera (Next Header , 8 bits). Identifica el tipo de la cabecera que sigue inmediatamente después de la cabecera IPv6 (es decir, en los primeros bytes del campo de datos del datagrama IPv6). Utiliza los mismos valores que el campo de Protocolo de la cabecera IPv4.

Límite de Saltos (8 bits). Entero sin signo que contendrá un valor que se decrementará en 1 unidad en cada nodo que reenvíe el datagrama. El datagrama se descartará cuando se llegue a cero. Similar al campo TTL de los datagramas IPv4.

Dirección IP de Fuente (128 bits)

Dirección IP de Destino (128 bits). Puede ser que no coincida con el destino final de la información, como pasa, por ejemplo, en el caso de que se incluya una cabecera de encaminamiento.

C. Asignación de direcciones IPv6

[32, p. 179] La IANA es la organización encargada de distribuir el espacio de direcciones de IPv6. Su función principal es la asignación de grandes bloques a los RIR, que serán los encargados de asignar bloques de Internet a los proveedores locales.

Las direcciones IPv6 se asignan a las organizaciones en bloques mucho mayores que los de direcciones IPv4. Las asignaciones recomendadas proporcionan un prefijo de red de 48 bits, lo cual deja 80 bits para la distribución de hosts en cada una de las subredes.

Debido al formato de número tan grande que utiliza IPv6, se asegura que prácticamente siempre haya direcciones disponibles y, por tanto, el uso de NAT se convierte en innecesario. Recordemos que NAT apareció para evitar el rápido agotamiento de las direcciones IPv4.

En la actualidad, solo está disponible la octava parte del total del espacio de direccionamiento IPv6. El resto de direcciones están reservadas para su futuro uso.

D. Direcciones especiales

[32, p. 179] Las direcciones IPv6 se clasifican en dos grandes grupos:

Direcciones unicast : son las que van dirigidas a una única interfaz de red.

Direcciones multicast : son las que van dirigidas a un grupo de interfaces de red. El formato de estas direcciones supone colocar el primer byte a 11111111, por tanto este tipo de direcciones siempre empezarán por FF. No se puede utilizar nunca una dirección multicast como origen.

Dentro de las direcciones unicast existen algunas especiales que no deben utilizarse nunca:

La dirección de loopback 0:0:0:0:0:0:0:1, que también puede expresarse como ::1/128

La dirección con todos sus bits a 0, expresada como ::/128 y que recibe el nombre de dirección indefinida . Al igual que en IPv4, esta dirección se usa por las interfaces cuando aún no se conoce la dirección IP real de la propia interfaz

La dirección local única, expresada como fc00::/7. Su uso es similar al de las direcciones privadas de IPv4

Dentro de las direcciones multicast, la dirección ff00::0/12 reservada por la IANA. Esta no debe ser utilizada por ningún grupo multicast.

E. Conversión de bits a hexadecimal

[32, p. 177] Para convertir bits a hexadecimales, cada cuatro bits se sustituyen por el número correspondiente según la tabla:

TABLA III CONVERTIR BITS A HEXADECIMAL [32]

Binario	Hexadecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

1.4.3. Mecanismos de transición

[31, p. 37] La migración natural de los sistemas en versión IPv4 a versión IPv6 será un proceso progresivo de adaptación. Hasta la extinción absoluta de IPv4 (que supondrá décadas de tiempo), existirán métodos llamados de transición que permitirán la coexistencia de ambas versiones del protocolo IP. En función de cada necesidad se optará por uno u otro y aunque existen múltiples alternativas, todas ellas pueden englobarse en una de las tres categorías que se detallan en los sucesivos apartados.

A. Dual Stack

[31, p. 37] «Dual stack» (traducción literal «doble pila») significa que el nodo tiene la capacidad de utilizar IPv4 e IPv6 al mismo tiempo. Para ello tendrá direcciones de ambas versiones y será capaz de comunicarse con otros nodos con protocolos en IPv4 y en IPv6. Es lo que se conoce como IPv4 e IPv6 nativo.

En el caso de un «host» con doble direccionamiento, éste enviará solicitud de DNS de una versión y en caso de no recibir respuesta, intentará validar solicitud en la otra versión. Según tecnología y fabricante, en unos casos se hace primero una solicitud en IPv6 y en otros se intenta primero lanzar una solicitud en IPv4.

En el caso de un «router», «Dual Stack» requiere que todas las interfaces conectadas tengan direccionamiento IPv6 y que éste se encamine con protocolos IPv6. Por lo general, la topología y diseño de red serán muy similares a los de IPv4 ya existentes.

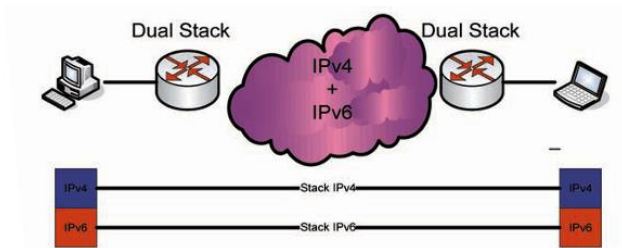


Fig. 4 Topología del Mecanismo Dual Stack [31]

```
Router0>en
Router0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router0 (config)#ipv6 unicast-routing
Router0 (config)#int fa 0/0
Router0 (config-if)#ipv6 enable
Router0 (config-if)#ip address 192.168.1.1 255.255.255.0
Router0 (config-if)#ipv6 address 2001:1:a:1::1/64
Router0 (config-if)#no shut
```

Fig. 5 Configuración del mecanismo Dual Stack [34]

B. Túneles de transición

[31, p. 38] Una opción con menor impacto en nuestra red es utilizar túneles de transición, que encapsulan una versión de IP y la transportan sobre la otra. Se han definido túneles para ambos casos, encapsular IPv6 en una red de IPv4, y encapsular IPv4 en una red IPv6. Mientras la primera dará conectividad en redes ya desplegadas, la segunda servirá como solución a nuevas redes IPv6 que necesiten mantener alguna conectividad en IPv4.

Ambos casos serán resolutivos si bien las necesidades de evolución de IP han hecho que se desarrollen muchos más métodos de tunelización de IPv6 sobre IPv4, como veremos en los ejercicios prácticos.

El mecanismo de un túnel consiste en convertir el paquete de la versión a transportar extremo a extremo en el “payload” o datos de la versión que tiene comunicación en todos los nodos intermedios. De este modo comunicamos islas aisladas de un protocolo como se indica en la siguiente ilustración.



Fig. 6 Topología del Mecanismo Tunelización [31]

En este caso, podemos conectar redes de IPv6 separadas entre sí utilizando la tecnología de IPv4 ya existente. Para la comunicación extremo a extremo en IPv6 la red IPv4 es transparente. Al mismo tiempo, IPv4 transporta el paquete de IPv6 encapsulado de forma que lo trata como información de datos del nivel superior y que por tanto será des encapsulada cuando llegue al destino. Por último, los nodos que interconectan redes de ambas versiones han de tener la capacidad de funcionar en modo «dual stack», para poder comunicarse con cada segmento de red como éste requiera. Existen diferentes tipos de túnel, pero todos ellos pueden dividirse en dos grandes categorías.

Los túneles punto a punto y los túneles punto a multipunto. Los primeros conectan únicamente a dos nodos, estableciendo un enlace virtual entre ambos, y se configuran de forma estática ambos extremos. En el caso de los túneles multipunto un nodo inicial es capaz de comunicarse mediante túnel con múltiples destinos remotos que también soporten el establecimiento de dicho túnel.

En este caso no es necesario preconfigurar de antemano el extremo remoto, sino que se descubre de forma dinámica, por tanto, es un diseño más escalable y que requiere de menos configuración, pero a efectos prácticos no difiere técnica ni conceptualmente de un túnel estático.

Generalmente, un túnel estático es preferible para tráfico continuo, para los que merezca la pena configurar un protocolo de encaminamiento IGP. Un túnel dinámico es más ligero y es adecuado para tráfico con poca frecuencia o poco predecibles.

[32, p. 180] La principal diferencia entre ellas radica en la ubicación de los nodos duales: si se colocan antes de la red IPv4, entre los dispositivos de red IPv4, etc.

B.1 Túnel 6to4

[29, p. 20] 6to4 es un túnel automático definido en la RFC 3056 que tiene como objetivo conectar dominios IPv6 a través de dominios IPv4. El dominio IPv6 que usa este mecanismo es llamado dominio 6to4. 6to4 define un modo específico de usar las direcciones IPv4 para construir las direcciones IPv6 que usará el dominio 6to4.



Fig. 7 Estructura de las direcciones del mecanismo de tunelización 6to4 [29]

2002::/16 es el espacio de direcciones reservado para 6to4, V4ADDR es la representación hexadecimal de la dirección pública IPv4 de la interfaz donde se desea habilitar 6to4 y el resto de los campos poseen el mismo significado explicado en epígrafes anteriores.

Como se puede apreciar, 6to4 permite asignar direcciones IPv6 y alcanzar hosts localizados en la Internet IPv6 sin necesidad de obtener un prefijo de dirección IPv6 global de un ISP.

Con la utilización de este mecanismo, el tráfico IPv6 es enviado a través de redes IPv4 comunicando redes aisladas que utilizan 6to4.

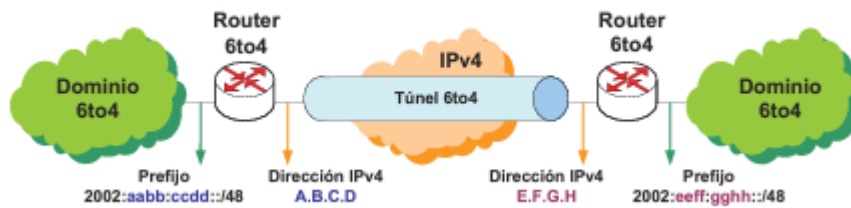


Fig. 8 Estructura del mecanismo de tunelización 6to4 [29]

Los paquetes IPv6 que posean direcciones de destino con un prefijo diferente al 2002:V4ADDR::/48 utilizado en su dominio 6to4, son encaminados hacia el router de borde y encapsulados en paquetes IPv4. Seguidamente son enviados a través de la red IPv4 para luego ser des encapsulados en el router de borde perteneciente al extremo final del túnel.

Al implementar este tipo de túnel, los dominios 6to4 pueden comunicarse sin necesidad de ninguna configuración adicional ni de la implementación de ningún protocolo de enrutamiento extra ya que de esto se encarga la red IPv4. Cuando un dominio 6to4 desea comunicarse con un dominio IPv6 no 6to4 se debe usar un relay 6to4, que no es más que un router con una interfaz conectada al dominio 6to4 y otra conectada a la red IPv6. La Fig. 11 muestra un túnel 6to4 que utiliza un router relay 6to4.

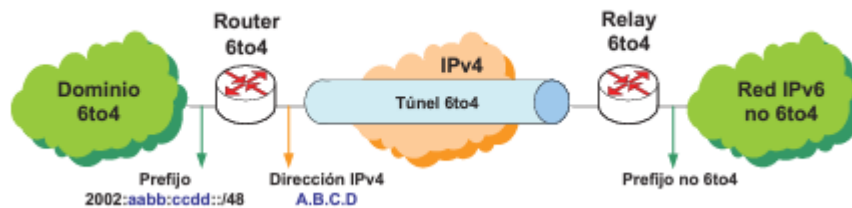


Fig. 9 Estructura del Mecanismo de Tunelización 6to4 con un router relay 6to4 [29]

El router de borde debe tener una ruta por defecto apuntando hacia la dirección del relay 6to4, mientras que este último debe tener una ruta por defecto hacia la Internet IPv6. Los paquetes IPv6 enviados a direcciones con prefijo diferente al correspondiente a 6to4, serán encapsulados y enrutados hacia el relay debido a la ruta por defecto. Luego el relay lo desencapsula y lo enruta hacia la red correspondiente. Adicionalmente, la RFC 3068 propone el uso de direcciones anycast para descubrir el relay 6to4 más cercano de manera automática. Para ello se ha reservado la dirección IPv4 anycast 192.88.99.1, que se debe configurar como dirección secundaria en los relays 6to4 en la interfaz de cara a la red IPv4. En este caso debe configurarse la dirección anycast antes mencionada como ruta por defecto en el router de borde.

El router de borde debe tener una ruta por defecto apuntando hacia la dirección del relay 6to4, mientras que este último debe tener una ruta por defecto hacia la Internet IPv6. Los paquetes IPv6 enviados a direcciones con prefijo diferente al correspondiente a 6to4, serán encapsulados y enrutados hacia el relay debido a la ruta por defecto. Luego el relay lo desencapsula y lo enruta hacia la red correspondiente. Adicionalmente, la RFC 3068 propone el uso de direcciones anycast para descubrir el relay 6to4 más cercano de manera automática. Para ello se ha reservado la dirección IPv4 anycast 192.88.99.1, que se debe configurar como dirección secundaria en los relays 6to4 en la interfaz de cara a la red IPv4. En este caso debe configurarse la dirección anycast antes mencionada como ruta por defecto en el router de borde.

TABLA IV CONFIGURACIÓN DEL MECANISMO DE TUNELIZACIÓN 6TO4 [35]

```
R1(config)#interface g0/1
R1(config-if)# ipv6 address 2002:C0A8:0500::5/64
R1(config)#interface g0/0
R1(config-if)# ipv6 address 2002:C0A8:0300::3/64
R1(config)#interface tunnel 1
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2002:C0A8:0300:0001::3/64
R1(config-if)#tunnel source 192.168.34.3
R1(config-if)#tunnel mode ipv6ip 6to4
R1(config-if)#ipv6 route 2002::/16 tunnel 1
```

B.2 Túnel ISATAP (Intra Site Automatic Tunnel Addressing Protocol)

[29, p. 23] Este tipo de túnel automático requiere que los nodos sean doble pila. Fue diseñado para crear túneles entre un host y un router o entre hosts pertenecientes al mismo sitio, al encapsular los datagramas IPv6 en los datagramas IPv4. Se encuentra descrito en la RFC 5214. El formato de las direcciones ISATAP. Los primeros 64 bits están constituidos por el prefijo fe80::/64 para las direcciones de enlace local. En el caso de las direcciones globales se debe escoger, para el uso de ISATAP, un /64 perteneciente al /48 asignado al sitio por parte de algún ISP. El identificador de la interfaz está dividido a la mitad. La IANA designó que los primeros 32

bits sean siempre 0000:5efe y los últimos 32 bits contienen la dirección IPv4 del nodo, ya sea pública o privada.

Fe80::/64(ENLACE LOCAL) Ó PREFIJO /64 (GLOBAL)	0000:5efe	Dirección IPv4
64 bits	32 bits	32 bits

Fig. 10 Formato de las direcciones del mecanismo de tunelización ISATAP [29]

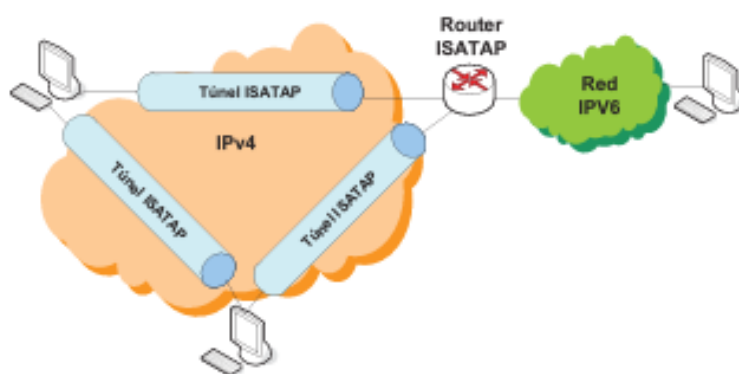


Fig. 11 Topología del mecanismo de tunelización ISATAP [29]

Los nodos ISATAP crean sus direcciones de enlace local basándose en su dirección IPv4 como ya ha sido descrito, con lo cual se establece un enlace virtual basado en las direcciones de enlace local.

En cuanto a las direcciones globales, en el caso de los routers debe ser configurada manualmente para que luego estos anuncien el prefijo /64 destinado para ISATAP y los hosts puedan conformar sus propias direcciones globales con la información anunciada más su dirección IPv4. En este caso también se conforma un enlace virtual entre los nodos, pero basado en direcciones globales.

Para la comunicación entre hosts ISATAP se utiliza el túnel ISATAP host-host. La encapsulación y desencapsulación de los paquetes la realizan siempre los hosts. Cuando un host ISATAP desea alcanzar un host perteneciente a una red IPv6 nativa se utiliza el túnel ISATAP entre host-router. La dirección del router por defecto para alcanzar la Internet IPv6 debe ser configurado manualmente en el host. Cuando el paquete llega al router es desencapsulado para luego ser encaminado utilizando técnicas de enrutamiento propias de IPv6. Este mecanismo no es apropiado para proveedores de servicio, sino para el uso interno

de empresas. Es importante aclarar que no debe hacerse uso de NAT (Network Address Translator) en el camino entre los nodos ISATAP.

b.2.1 Ejemplo del mecanismo de tunelización ISATAP

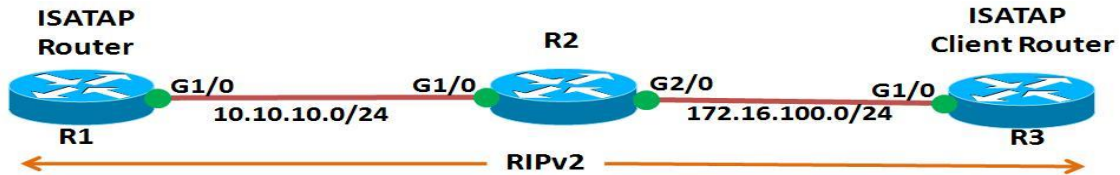


Fig. 12 Ejemplo del mecanismo de tunelización ISATAP [36]

Configuración del ejemplo del mecanismo de tunelización ISATAP

TABLA V CONFIGURACIÓN R1 [36]

```
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Tunnel1
no ip address
no ip redirects
ipv6 address 2001:DB8:AA10:10::/64 eui-64
no ipv6 nd ra suppress
tunnel source Loopback0
tunnel mode ipv6ip isatap
!
interface GigabitEthernet1/0
ip address 10.10.10.100 255.255.255.0
negotiation auto
!
router rip
version 2
network 1.0.0.0
network 10.0.0.0
!
gatekeeper
shutdown
!
!
end
```

TABLA VI CONFIGURACIÓN R2 [36]

```
hostname R2
!
ip source-route
ip cef
!
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
!
interface Loopback1
ip address 2.2.2.3 255.255.255.255
!
interface GigabitEthernet1/0
ip address 10.10.10.101 255.255.255.0
negotiation auto
!
!
interface GigabitEthernet2/0
ip address 172.16.100.1 255.255.255.0
negotiation auto
!
router rip
version 2
network 2.0.0.0
network 10.0.0.0
network 172.16.0.0
!
!
!
end
```

**TABLA VIII CONFIGURACIÓN R3 (ISATAP
CLIENTE ROUTER) [36]**

```
!  
!  
version 15.0  
!  
hostname R3  
!  
ip source-route  
ip cef  
!  
interface Loopback0  
ip address 3.3.3.3 255.255.255.255  
!  
!  
interface Tunnel1  
no ip address  
ipv6 address autoconfig  
ipv6 enable  
tunnel source GigabitEthernet1/0  
tunnel mode ipv6ip  
tunnel destination 1.1.1.1  
!  
  
interface GigabitEthernet1/0  
ip address 172.16.100.2 255.255.255.0  
negotiation auto  
!  
!  
router rip  
version 2  
network 3.0.0.0  
network 172.16.0.0  
!  
!  
!  
end
```

**TABLA VII PING ENTRE ROUTER
ISATAP Y CLIENTE [36]**

Ahora el enrutador ISATAP debería poder hacer ping al cliente, es decir, el enrutador R3

```
R1 # ping 2001: DB8: AA10: 10 ::  
AC10: 6402
```

Escriba la secuencia de escape para abortar.

```
Enviando 5 ICMP Echos de 100  
bytes a 2001: DB8: AA10: 10 ::  
AC10: 6402, el tiempo de espera es  
de 2 segundos
```

C. Túnel 6rd (IPv6 Rapid Deployment on IPv4 Infrastructures)

[29, p. 28]6rd es un túnel automático definido en las RFC 5569 y RFC 5969. Fue diseñado para acelerar el despliegue de IPv6 en los usuarios finales conectados a infraestructuras de redes IPv4.

Este mecanismo es muy similar a 6to4, con la diferencia que utiliza un prefijo IPv6 propio del ISP en lugar del utilizado para 6to4. De esta manera, el dominio operacional está limitado al ISP y se encuentra bajo su directo control. El prefijo a utilizar para el dominio 6rd será seleccionado por el ISP.

Dentro del dominio 6rd existen 6rd CE (Customer Edge) routers y 6rd BR (Border Relays). Los paquetes IPv6 encapsulados viajan dentro de la estructura de red del ISP y son enrutados por ambos tipos de routers. Los 6rd BR solo son atravesados cuando se requiere la comunicación con hosts externos al dominio 6rd del ISP.

El prefijo para ser utilizado en un sitio es creado al combinar el prefijo 6rd y toda o parte de la dirección IPv4 del CE. Es decir, que el prefijo, así como la posición y el número de bits a utilizar de la dirección IPv4 varían de un dominio 6rd a otro. 6rd permite que el ISP ajuste el tamaño del prefijo: cuántos bits serán utilizados por el mecanismo 6rd y cuántos serán delegados a los sitios.

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **tunnel source** *{ip-address| interface-t type interface-number}*
5. **tunnel mode ipv6ip** [**6rd** | **6to4** | **auto-tunnel** | **isatap**]
6. **tunnel 6rd prefix** *ipv6-prefix / prefix-length*
7. **tunnel 6rd ipv4** *{prefix-length length} {suffix-length length}*

Fig. 13 Formato del mecanismo de tunelización 6RD [37]

```

interface Tunnell
  ipv6 address 2001:B000:100::1/32
  tunnel source loopback 1
  tunnel mode ipv6ip 6rd
  tunnel 6rd prefix 2001:B000::/32
  tunnel 6rd ipv4 prefix-len 16 suffix-len 8
end
Router# show tunnel 6rd tunnel 1
Interface Tunnell:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
  V4 Common Prefix Length: 16, Value: 10.1.0.0
  V4 Common Suffix Length: 8, Value: 0.0.0.1

```

Fig. 14 Ejemplo de configuración del Mecanismo 6RD [37]

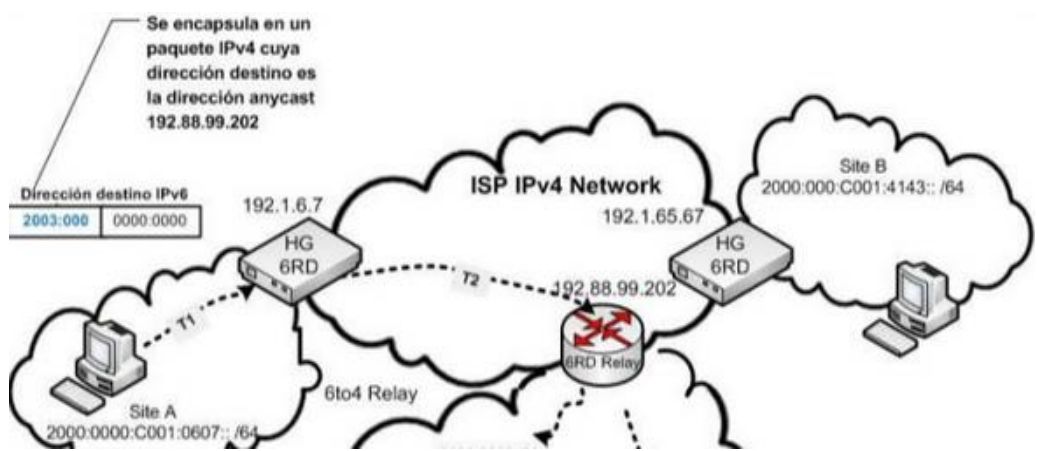


Fig. 15 Estructura del Mecanismo de Tunnelización automática 6RD [31]

D. Túnel Manual IPV6IP

[29, p. 30] Los túneles manuales son usados generalmente para comunicar redes doble pila que utilizan un backbone IPv4. En estos casos las configuraciones se implementan en los routers de borde de cada una de estas redes, los cuales realizan la encapsulación y desencapsulación de los paquetes. Se debe realizar la configuración en ambos extremos para lograr la comunicación bidireccional.

Este tipo de túneles solo es conveniente cuando no sea necesario interconectar muchos puntos ya que la configuración manual de los mismos podría resultar trabajosa. En esos casos se recomienda utilizar mecanismos automáticos.

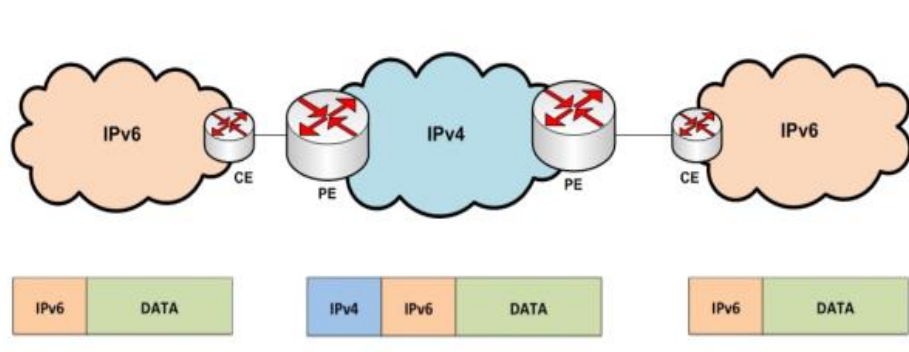


Fig. 16 Estructura del mecanismo Túnel Manual IPv6IP [38]

Configuración de túnel manual:

[31, p. 77] Para configurar un túnel manualmente es necesario definir una interfaz túnel. Es una interfaz lógica que se asocia a una dirección IP que se utilizará como interfaz de salida para el tráfico encapsulado. En este ejemplo encapsulamos tráfico IPv6 sobre IPv4, por tanto, la interfaz túnel la asociamos a una interfaz «loopback» que tiene dirección IP de IPv4. El destino del tráfico encapsulado en la red IPv4 será una dirección del destino del túnel alcanzable en IPv4. Como es un túnel manual, la especificamos de forma explícita. Además, es necesario configurar el tipo de encapsulación que realiza el túnel, para el caso de un túnel manual es «ipv6ip». Por último, para que la comunicación sea posible, es necesario hacer que la interfaz túnel sea visible en la topología de la isla en IPv6. Para ello se configura una dirección IPv6 y permitimos su anuncio en la red, en este caso implementando OSPFv3.

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix / prefix-length [eui-64]*
5. **tunnel source** *{ip-address | interface-type interface-number}*
6. **tunnel destination** *ip-address*
7. **tunnel mode ipv6ip**

Fig. 17 Formato del mecanismo Túnel Manual IPv6IP [39, p. 5]

E. Traducción de direcciones de red mediante NAT

[31, p. 40] En los dos casos anteriores existe una característica común y es que permiten la comunicación entre nodos que soportan la misma versión de IP, tanto la versión 4 como la versión 6. Pero se puede dar la situación en la que necesitemos permitir que un nodo en una versión envíe tráfico a otro nodo que tenga una versión IP diferente. Para que este escenario pueda funcionar debemos realizar la traducción de un protocolo a otro y para ello se ha recurrido a una tecnología ampliamente utilizada en IPv4 para traducir el direccionamiento privado en público y viceversa conocida como NAT 17 («Network Address Translation»).

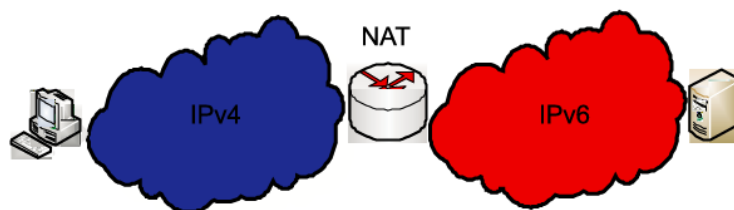


Fig. 18 Estructura del mecanismo de traducción NAT [29]

Para el caso de IPv6 se han desarrollado diversas versiones de NAT, como NAT-PT 18 («Network Address Translation - Protocol Translation») que no sólo traduce las direcciones de IPv4-IPv6 sino también las cabeceras de ambos protocolos, así como las de UDP/TCP o ICMP/ICMPv6. El uso de NAT plantea una problemática para niveles de capa superior que requieran el uso de la dirección IP (como por ejemplo FTP, DNS o VoIP). Por ello es necesario aplicarse junto con los llamados ALG («Application Layer Gateways») que soportan esas funciones. Actualmente esta versión se considera obsoleta debido a sus limitaciones, pero sigue siendo útil para fines académicos.

Ante las limitaciones de NAT-PT se desarrolló otra versión conocida como NAT64 20, que por su complejidad para aplicarse a un entorno de simulador virtual, no será contemplada en este tomo. Junto con las funciones de NAT, el «router» de interconexión de ambas versiones ha de garantizar la disociación de solicitudes de DNS entre DNSv4 y DNSv6.

Más adelante se analizan los distintos tipos de NAT-PT que se pueden aplicar, como por ejemplo NAT estático, NAT dinámico y PAT («Port Address Translation»). [40]

1. NAT dinámico

[40]El NAT dinámico es el más básico de todos los métodos de traducción de direcciones privadas a públicas. Consiste en tener un bloque IP público e ir asignando dinámicamente una de esas IP a cada máquina de la LAN interna para que salga a Internet. Si tenemos 3 máquinas en nuestra LAN, como la imagen, necesitaremos entonces 3 IP públicas extra (aparte de la necesaria en la interfaz WAN del router) para lograr conectividad. En este tipo de NAT, las IP reservadas para el bloque público se van utilizando y se crea un mapping 1:1 entre las IP internas y las externas. Si definimos solo 3 IP públicas entonces solamente podrán conectarse 3 máquinas internas hacia Internet. Esta asociación se crea en forma dinámica.

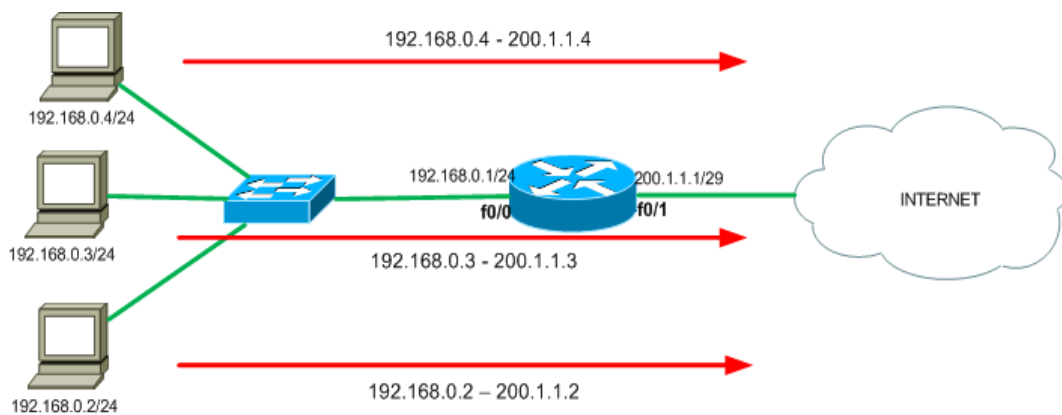


Fig. 19 Ejemplo del mecanismo de Traducción NAT Dinámico [40]

Configuración de NAT dinámico:

```
Router(config)# ip nat pool RANGOPUBLICO 200.1.1.2 200.1.1.4 netmask
255.255.255.248
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool RANGOPUBLICO
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface FastEthernet0/1
Router(config-if)# ip nat outside
```

2. NAT estático

[40] El NAT estático es el más simple de configurar y permite asociar estáticamente una dirección pública a una dirección IP privada. Es ideal para permitir el acceso desde Internet a un servidor que alojamos en una DMZ por ejemplo o en la red LAN institucional.

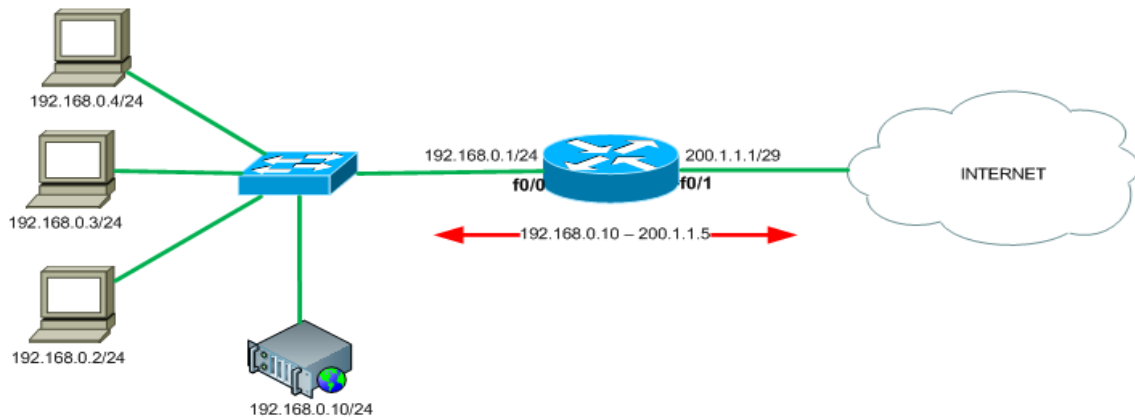


Fig. 20 Ejemplo del mecanismo de Traducción NAT estático [40]

En nuestra LAN se ha instalado un servidor Web al cual se le ha asignado la dirección IP privada 192.168.0.10, pero es requisito que desde Internet también se pueda acceder. Ya que tenemos direcciones IP privadas, este servidor no puede ser alcanzado desde una red pública, por lo tanto creamos una forma de asociar una dirección IP pública única al servidor. Aquí hemos asignado la IP 200.1.1.5/29. Esta IP no puede ser utilizada en otro NAT al mismo tiempo ya que queda reservada para la IP 192.168.0.10. En otros sistemas, como OpenBSD, se suele utilizar el nombre de NAT 1:1 (one-to-one).

Configuración de NAT estático:

```
Router(config)# ip nat inside source static 192.168.0.10 200.1.1.5
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface FastEthernet0/1
Router(config-if)# ip nat outside
```

1.4.4 Etapas de migración

Según [6] si las empresas adoptan una estrategia de migración a IPv6, esta consiste de 3 etapas:

La primera etapa es instalar un Gateway para proveer una transición suave entre los dos estándares. La segunda etapa involucra la construcción de la infraestructura de la red mientras que la última etapa es hacer que las aplicaciones funcionen en IPv6.

El proceso de migración puede tomar de algunos meses a algunos años. La solución intermedia es usar un Gateway que permita a las empresas continuar usualmente con sus negocios mientras les da el tiempo de construir una nueva infraestructura y reescribir las aplicaciones para que funcionen en IPv6.

Esto permite que las empresas tengan la libertad de probar, mover y migrar su infraestructura existente a un paso controlado administrado, da a la compañía la oportunidad de migrar sus clientes o servidores a redes IPv6 sin tener que cambiar todo en un paso.

Existen dos posibles escenarios para una estrategia de migración suave y controlada. Las empresas pueden mover los clientes hacia IPv6 mientras mantienen sus servidores en IPv4 o pueden migrar los servidores a IPv6 y dejar a sus clientes en un ambiente IPv4. Mover el cliente a IPv6 requiere que todos los clientes sean capaces de agregarse a la red vía caminos IPv6 permitidos.

Muchas empresas encontrarán más fácil comenzar a migrar servidores (aplicaciones) antes que los dispositivos cliente, esto simplemente porque los servidores están completamente bajo el control de las empresas mientras que los dispositivos clientes a menudo no lo están. Al migrar servidores, el dispositivo Gateway se encuentra entre los servidores y los clientes, y debe agregarse una red capaz de soportar IPv6. El resultado es que la red tendrá IPv4 sobre el lado del cliente del dispositivo y ambos protocolos IPv4 e IPv6 detrás de él.

Una vez que la red IPv6 es establecida, los servidores pueden moverse de la red IPv4. Dado que los dispositivos cliente en un futuro estarán basados en IPv6, es imperativo que las empresas se aseguren que su infraestructura y aplicaciones también sean capaces de soportar IPv6.

II.- Método de Investigación

Las fases para realizar esta investigación fueron planteadas en [41]. El cual tiene como objetivo proveer un marco para llevar a cabo el desarrollo de la revisión bibliográfica de un tema específico de forma concisa, válida y justificable. A continuación, se realiza una descripción del método mencionado en la Figura 21.



Fig. 21 Método de revisión bibliográfica

Fuente: Elaboración propia basado en [41]

2.1 Plan de investigación

En esta etapa de la investigación se desarrolló lo siguiente:

- Interrogantes de investigación que el estudio responderá
- Protocolo de revisión que se seguirá para la búsqueda de la información

2.1.1 Interrogantes de la investigación

Se realizó la formulación de cuatro preguntas que serán respondidas con los artículos recopilados.

- 1.- ¿Existe alguna otra solución haciendo uso del mecanismo de tunelización?
- 2.- ¿Se muestran etapas claras para realizar la migración de IPv4 a IPv6?
- 3.- ¿Qué tipo de seguridad se podrían implementar en los mecanismos de transición?
- 4.- ¿Qué mecanismos de transición se implementaron?

2.1.2 Protocolo de revisión

Para realizar la revisión se hizo uso de la plataforma SCImago Journal & Country Rank el cual se exploró el ranking de Journals. En el campo de áreas se seleccionó Computer Science; en la categoría se selecciona Computer Networks and Communications debido a que la presente investigación está relacionada al tema de redes informáticas. Luego de

haber filtrado se mostrará los journals en un Ranking. Se seleccionó la base de datos IEEE debido a que los primeros journals no se encontró artículos del tema que abarca esta investigación. Además de diseñar la regla de búsqueda que se enfoca al objetivo de la investigación.

The screenshot shows the Scimago Journal & Country Rank interface. The 'Computer Science' and 'Computer Networks and Communications' dropdown menus are highlighted with a red box. Below the filters, there are checkboxes for 'Only Open Access Journals', 'Only ScieLo Journals', and 'Only WoS Journals'. A search bar is visible at the top right with the placeholder text 'Enter Journal Title, ISSN or Publisher Name'. The main table displays journal rankings with columns for Title, Type, SJR, H index, Total Docs. (2018), Total Docs. (3years), Total Refs. (2018), Total Cites (3years), Citable Docs. (3years), Cites / Doc. (2years), and Ref. / Doc. (2018).

Title	Type	SJR	H index	Total Docs. (2018)	Total Docs. (3years)	Total Refs. (2018)	Total Cites (3years)	Citable Docs. (3years)	Cites / Doc. (2years)	Ref. / Doc. (2018)
1 npj Quantum Information	journal	3.929 Q1	18	5	59	272	499	56	9.32	54.40
2 31st International Conference on Machine Learning, ICML 2014	conference and proceedings	3.849	28	0	90	0	1583	89	0.00	0.00

Fig. 22 Campos seleccionados para filtrar Journals [42]

The screenshot shows a list of IEEE journals in the Scimago Journal & Country Rank interface. The table displays journal rankings with columns for Title, Type, SJR, H index, Total Docs. (2018), Total Docs. (3years), Total Refs. (2018), Total Cites (3years), Citable Docs. (3years), Cites / Doc. (2years), and Ref. / Doc. (2018).

11 IEEE Communications Magazine	journal	2.373 Q1	213	353	1106	4455	12402	934	12.73	12.62
12 Information Systems Journal	journal	2.319 Q1	79	63	90	5126	561	71	6.16	81.37
13 IEEE Journal on Selected Areas in Communications	journal	2.294 Q1	211	217	741	7883	8083	715	11.55	36.33
14 IEEE Transactions on Control of Network Systems	journal	2.098 Q1	28	230	157	6207	899	154	5.51	26.99
15 Proceedings - IEEE Symposium on Security and Privacy	conference and proceedings	1.890	97	66	120	3574	1349	115	9.50	54.15
16 IEEE Network	journal	1.771 Q1	111	106	262	1484	2342	238	9.59	14.00

Fig. 23 Selección de IEEE [42]

2.2 Procedimiento de la investigación

2.2.1 Identificar las investigaciones relevantes

Para identificar las investigaciones relevantes se hizo uso de una regla de búsqueda que consta de 7 palabras claves. Luego de que se mostraran los resultados se analizó si se implementan los mecanismos de transición para la migración de una red IPv4 a una red IPv6. Al finalizar este análisis se seleccionó 59 artículos.

TABLA IX BÚSQUEDA DE BASE DE DATOS Y RESULTADOS

N°	Base de datos	Regla de búsqueda	Resultados
1	IEEE Xplore Digital Library	(((((Transition mechanisms) AND IPv6) AND IPv4) AND Transition strategies) AND Tunneling mechanisms) AND Translation mechanisms) AND Dual Stack)	59

Fuente: Elaboración propia

The screenshot shows the IEEE Xplore Digital Library search interface. At the top, there are navigation links for IEEE.org, IEEE Xplore Digital Library, IEEE-SA, IEEE Spectrum, and More Sites. The main header includes the IEEE Xplore logo and an Institutional Sign In button. Below the header, there are navigation tabs for Browse, My Settings, Get Help, and Subscribe. A search bar is present with a dropdown menu set to 'All' and a search button. Below the search bar, there are options for Advanced Search and Other Search Options. The search results section shows 'Search within results' and 'Per Page: 25'. The search query is displayed as 'Displaying results 1-25 of 203 for ((((((Transition mechanisms) AND IPv6) AND IPv4) AND Transition strategies) AND Tunneling mechanisms) AND Translation mechanisms) AND Dual Stack))'. Below the query, there are checkboxes for filtering results by type: Conferences (77), Standards (50), Books (43), Magazines (17), and Journals (16).

Fig. 24 Regla de Búsqueda

Fuente: Elaboración propia

2.2.2 Sintetizar los datos

En esta etapa se realizó el análisis de las palabras claves de cada artículo en el que se hace uso de INSPEC, esta es una base de datos de indexación científica y técnica. Como resultado final será una tabla que consta de los siguientes campos: título de la publicación, autor, año de la publicación, palabras clave del autor, términos de IEEE, términos controlados y no controlados por INSPEC, número de citas y referencias de cada publicación.

Tabla X Sintetizar los datos

N°	Título del documento	Autores	Año	Palabra clave del autor	Términos de IEEE	Términos controlados por INSPEC	Términos no controlados por INSPEC	# de citas	# Referencias
1	DTTS: A Transparent and Scalable Solution for IPv4 to IPv6 Transition [8]	Kai Wang, Ann-Kian Yeo, A. L. Ananda	2001	Interoperability, IPv4, IPv6, Transition, Dynamic Tunneling, Dual Stack.	Tunneling, IP networks, Routing, Protocols, Web and internet services, Computer networks, Network address translation, Proposals, Reliability, Prototypes	protocols , Internet , open systems , telecommunication network routing	IPv4 Internet , IPv6 network deployment , interoperability, dynamic tunneling transition solution, routing, DNS, error handling , dual stack approach, packet encapsulation, transparent transition, scalable transition, protocols	3	19

2	Deploying IPv6 [9]	Alain Durand	2001		Internet, Network address translation, Application software, Operating systems, Investments, Protocols, Space technology, IP networks, Hardware, Switches	Internet, transport protocols	IPv6, Internet Protocol, IPv4, specifications, IETF	12	0
3	Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version 4 (IPv4) Tunnel [10]	M. Samad, F. Yusuf, Habibah Hashimy Md Mahdz Md Zan	2002	Internet Protocol, IPv6, IPv4, Transition Tools, Tunneling, Encapsulation	Internet, Protocols, Tunneling, Encapsulation, Electronic mail, Telecommunication traffic, Proposals, Costs, Joining processes, Next generation networking	Internet, transport protocols, telecommunication computing, telecommunication network routing	Internet Protocol, IPv6, IPv4, transition tools, hybrid stack mechanism, internetwork infrastructure, tunnel broker, dual stack router	5	8
4	The IPv6 Transition [44]	Tricia Dunn	2002		Tunneling, Privacy, Network servers, Web server, Telecommunication traffic, Protocols,			5	0

					Internet , Routing, Unicast, Scattering				
5	Transition to IPv6 in GPRS and WCDMA Mobile Networks [11]	Juha Wiljakka, Nokia	2002		Intelligent networks, Ground penetrating radar, Multiaccess communication, IP networks, Internet, Protocols, Routing, GSM, Network servers, Explosives	packet radio networks, cellular radio, transport protocols, Internet, radio equipment, code division multiple access, broadband networks	IPv6, GPRS, WCDMA mobile networks, Internet address space size, Internet address space structure, interworking, IPv4 networks, IPv4 services, network/terminal equipment, transition methods, dual IPv4/IPv6 stacks, tunneling, translators, 2G/3G mobile network, mobile terminals, Internet Protocol version	6	10
6	An IPv4-to-IPv6 Dual Stack Transition Mechanism Supporting Transparent Connections between IPv6 [12]	Eun-Young Park, Jae-Hwoon Lee ; Eun-Young Park, Jae-Hwoon Lee	2004	IPv6, IPv4, Transition mechanism, 4to6 DSTM	Intelligent networks, Protocols, Internet, Network address translation, Network servers, Research and development,	IP networks, transport protocols, Internet	dual stack transition mechanism, IPv4 network, IPv6 network	7	15

	Hosts and IPv4 Hosts in Integrated IPv6/IPv4 Network				Routing, Security, Tunneling				
7	Performance Investigation of IPv4/IPv6 Transition Mechanisms [13]	Jiann- Liang Chen, Yao- Chung Chang and Chien- Hsiu Lin	2004	Ih.6 networks, transition mechanisms, IETF NGtrans, tunneling mechanisms, performance metrics	Protocols,Tunne ling, Delay , Throughput , Performance loss, Propagation losses, Computer science , Electronic mail ,Web and internet services, Next generation networking			3	18
8	IPv6 Integration and Coexistence Strategies for Next-Generation Networks [14]	Mallik Tatipamul a ,Patrick Grossetete , Hiroshi Esaki	2004		Next generation networking, Multiprotocol label switching, Web and internet services, IP networks, Spine, Space technology, Home appliances, Personal digital assistants, Network address translation, Transportation	Internet, multiprotoc ol label switching, transport protocols, IP networks	IPv6 integration, coexistence strategies, next-generation networks, IPv4 networks, deployment strategies, network design, service provider environments, multiprotocol label switching networks, Internet protocol	15	9

9	Managing the Co-existing Network of IPv6 and IPv4 under Various Transition Mechanisms [15]	I-Ping Hsieh ; Shang-Juh Kao	2005	IPv6, co-existing network, network management	Tunneling, Protocols, Environmental management, Telecommunication traffic, Information technology, Monitoring, Computer network management, Computer science, Internet, IP networks	IP networks, computer network management, protocols	IPv6 network management, IPv4 network management, transition mechanisms, network protocol, dual stack mechanism, tunneling mechanism, translation mechanism, co-existing network management	8	19
10	A Global Perspective of IPv6 Native and Transition Scenarios for DSL Infrastructures [16]	T. Camilo; S. Pasqualini	2006		DSL, Application specific processors, Guidelines, Asynchronous transfer mode, Research and development, Communications technology, Spine, Metropolitan area networks, Tunneling, IP networks	digital subscriber lines, IP networks, metropolitan area networks	IPv6 native scenarios, IPv6 transition scenarios, DSL infrastructures, digital subscriber lines, fixed-access multi-edged MAN, metropolitan area network, connectivity wholesale models, IPv4-IPv6 coexistence scenarios	0	20

11	New IPv6 Transition Mechanism based on End-to-End Tunnel [17]	SungBack Hong ; NamSeok Ko ; HoYong Ryu ; Nam Kim Chungbuk National University , 12 Gaeshin-Dong, Heungduk-gu, Chungbuk , 361-763, Korea. Email: namkim@chungbuk.ac.kr	2006		Tunneling, IP networks, Next generation networking, Web and internet services, Routing, Telecommunications, Costs, Scalability, Protocols, Spine	IP networks, telecommunication network routing	IPv6 transition mechanism, IPv4 network, end-to-end tunneling, IPv6 services		3
12	Implementation of IPv4 Over IPv6 Using Dual Stack Transition Mechanism (DSTM) on 6iNet [18]	H.M. Tahir ; A. Taa ; N.B.M. Nasir	2006	IPv4,IPv6, Transition Mechanism, DSTM	Protocols, Web and internet services, IP networks, Testing,Space technology, Personal digital assistants, Graphical user interfaces,	transport protocols	IPv4, IPv6, Internet protocol version four, Internet protocol version six,dual stack transition Mechanism, 6iNet	3	18

					Joining processes, Transportation, Automobiles				
13	AN APPROACH TO IPV6 TRANSITION IN WIRELESS NETWORKS [19]	Ed Jankiewicz ; Kwai Fung Chan ; David Green	2006		Wireless networks, Routing, Network address translation, IP networks, Prototypes, Costs, Testing, Mobile communication, Design engineering, Next generation networking	IP networks, military communication, open systems, radio networks	US Department of Defense, DoD, Internet protocol version 6, IPv6, interoperability, IPv4 network, US Army Communications, Electronics Research Development-Engineering Center, CERDEC Space-Terrestrial Communications Directorate, S&TCD, Next Generation Network, XGN, next-generation wireless network		22
14	An Approach for the Administration and Security of IPv6 Transition Mechanisms: An SNMP MIB for 6to4 [20]	Georgios Koutepas ; Athanasios Douitsis ; Demetris Philippides ; Vasilis Maglaris	2006		Tunneling, Network address translation, Information management, Databases, Multicast protocols, Relays, Computer security,	IP networks, telecommunication network management, telecommunication security,	IPv6 transition mechanisms, IP protocol, tunnelling functionality, 6to4, SNMP management information database	1	10

					National security, Computer network management, Engineering management	transport protocols			
15	IPv6 Solutions for NAT Overlap [21]	S. McFarland	2006		Network address translation, Peer to peer computing, Network servers, Corporate acquisitions, IP networks, Companies, Costs, Web server, File servers, Optimized production technology	computer network management, corporate acquisitions, IP networks	IPv6 solutions, NAT overlap, mergers and acquisitions, IP network, readdressing, network address translation overlap	1	8
16	An Empirical Analysis of IPv6 Transition Mechanisms [22]	Myung-Ki Shin ; Hyoung-Jun Kim ; D. Santay ; D. Montgomery	2006	IPv6, Transition Mechanism, Application	TCPIP, Tunneling, Protocols, Degradation, Internet, Ethernet networks, Encapsulation, NIST, Data communication,	IP networks, open systems	IPv6 transition mechanisms, interoperability, IPv4	3	15

					Security				
17	Enhancing Teredo IPv6 Tunneling to Traverse the Symmetric NAT [23]	Shiang-Ming Huang ; Quincy Wu ; Yi-Bing Lin	2006	IPv6, NAT, Teredo, tunneling IPv6, NAT, Teredo, tunneling	Tunneling, Network address translation, Relays, Network servers, Access protocols, Routing protocols, Telecommunication traffic, Web and internet services, Quality of service, Payloads	IP networks, transport protocols	Teredo IPv6 tunneling enhancement, network address translation, symmetric NAT, dual-stack node, private IPv4 network	2	4
18	Study of SIP-based VoIP Application Interworking with IPv4 - IPv6 Transitioning Mechanisms [24]	S. Tomic ; T. Hoehner ; R. Menedetter ; R. Maslenka ; M. Banfield ; R. Lauster	2006	SIP, IPv6, IP Transition	Internet telephony, Network servers, Next generation networking, IP networks, Payloads, Testing, Clouds, Transport protocols, Scalability, Performance analysis	Internet telephony, protocols	VoIP, interworking, IPv4-IPv6 transitioning mechanisms, networking, session initiation protocol	1	7

19	Migrating SIP-based Conversational Services to IPv6: Complications and interworking with IPv4 [45]	Mohamed Boucadair ; Yoann NOISETTE	2007	SIP , IMS , IPv6 , Migration, Coexistence.	Protocols , Telecommunications , Research and development , Peer to peer computing , Internet telephony , Routing , Manufacturing , Occupational stress, TV broadcasting , Technological innovation	Internet, telecommunication network routing, transport protocols	SIP-based conversational services,IPv6 infrastructures , call routing, signalling protocols	11	13
20	Performance Evaluation of SIPv6 Transitioning [25]	Thomas Hoehner ; Martin Petraschek ; Slobodanka Tomic ; Michael Hirschbichler	2007		Protocols , Internet telephony, Testing, Next generation networking, IP networks, Gain measurement, Broadband communication, Security , Standards development, Performance gain	Internet, Internet telephony, performance evaluation , signalling protocols, transport protocols	performance evaluation, SIPv6 transitioning, Internet,IPv6 protocol , interoperability, session initiation protocol, application layer protocol, voice-over-IP		9

21	Deployment Strategy and Performance Evaluation of the IPv6 Home Network using the Home Server [26]	Min Ho Park ; Jung Tae Kim ; Eui Hyun Paik	2007		Home automation , Network servers , Web server , IP networks , Consumer electronics , Explosives , Web and internet services , Tunneling , Performance evaluation , Testing	home automation , home computing , Internet , IP networks	home server , IPv6 home network , ubiquitous home network , consumer electronics , end-to-end connectivity , Internet , home-to-home tunneling , IPv4/6 transition mechanism , interoperability		5
23	A Novel IPv4/IPv6 Translation Mechanism Based on NAT-PT [46]	Wenming Shi ; Chuanhe Huang ; Qinggang Wang ; Yan Chen ; Yiming Huang ;	2007	NAT-PT , FTP-ALG , DNS-ALG ,	Routing , Unicast , Network servers , Protocols				9

		Yong Cheng		Translation Gateway , Transmission Layer Translation , Mobile Internet					
24	Security Mechanisms for the IPv4 to IPv6 Transition [47]	Abidah Hj Mat Taib ; Rahmat Budiarto	2007	IPv6 Transition , Dual stack , Tunneling , Security Mechanisms , Distributed Firewalls	Protocols , Tunneling , Web and internet services , Data security , Intrusion detection , IP networks , Research and development , Information filtering ,	authorisation , Internet , IP networks , telecommunication network routing , telecommunication security ,	security mechanisms , IPv4-IPv6 transition , Internet services , Internet protocols , dual-stacked host , packet filtering , edge router , host-based firewall	1	

					Information filters , Databases	transport protocols			
25	Bi-Directional Mapping System as a New IPv4/IPv6 Translation Mechanism [48]	Ra'ed AlJa'afreh ; John Mellor ; Mumtaz Kamala ; Basil Kasasbeh	2008	IPv4 , IPv6 , IPv4/IPv6 Address Mapping , BDMS.	Bidirectional control , Internet , IP networks , Protocols , Tunneling , Costs , Computer networks , Computational modeling , Computer simulation , Informatics			3	31
26	Performance Comparison of IPv4 and IPv6 on Various	Shaneel Narayan ; Samad S. Kolahi ;	2008	Internet Protocol	Operating systems	Internet	Windows operating system	14	22

	Windows Operating Systems [49]	Yonathan Sunarto ; Du D. T. Nguyen ; Paul Man		IPv4 , IPv6 , network performance , Windows operating system	Internet , Protocols , Payloads , Pervasive computing , Information technology , Degradation , Computer networks , Network servers , Telecommunication traffic	operating systems (computers) , transport protocols	IPv6 , Internet Protocol , IPv4 , IP stack , Microsoft operating system , Windows server 2003		
27	A new IPv6 Tunneling Protocol:Escort [50]	Hailin An ; Wanming Luo ; Xingfeng Li ; Xinchang Zhang ; Baoping Yan	2009		Tunneling , Protocols , Network address translation , Relays	IP networks , telecommunication security ,	IPv6 tunneling protocol , network address translations , NAT , UDP	1	12

					, Network servers , Security , Computer networks , Linux , IP networks , Quality of service	transport protocols	, Teredo , ID-locator , identity address , Escort relays , Linux , Miredo-relay		
28	IPv6 Security Challenges [51]	Carlos E. Caicedo ; James B.D. Joshi ; Summit R. Tuladhar	2009	IPv6 , IPv4 , network security , network attacks , IPSec , Internet Protocol	Protocols , Network address translation , Data security , Computer security , Space technology , IP networks ,	Internet , protocols , telecommu nication security	IPv6 , Internet protocol , security	20	9

					Communication system security , Information security , Authentication , Switches				
29	IPv4 to IPv6 Evolution Strategies of Pakistan Internet Exchange [52]	Asif Nawaz ; Mahmood Ashraf ; X. B. Hong ; J. Wu ; J. T. Lin	2009	IPv4 to IPv6 Evolution Strategies , IPv6 Migration Strategies , Pakistan Internet Exchange , PIE	Telecommunication traffic , Web and internet services , Telecommunication switching , Routing protocols , Educational institutions , Internet telephony , DSL	Internet , IP networks , telecommunication traffic , transport protocols	IPv4 , IPv6 , Pakistan Internet exchange point , telecommunication traffic , Pakistan telecommunication authority		10

					, IPTV , Optical fiber cables , Cities and towns				
30	An Overview of IPv4 to IPv6 Transition and Security Issues [53]	Muhammad Rizwan Sabir ; Muhammad Abuzar Fahiem ; Muhammad Saleem Mian	2009	Network security , IPSec , IPv4 , IPv6 , Transition mechanisms	Data security , Information security , Computer networks , Delay , Routing , Switches , Authentication , Intrusion detection , Mobile communication ,	IP networks , telecommunication security	IPv4 , IPv6 , security issues , transition mechanisms , network security , network expansions , security measures	5	37

					Mobile computing				
31	A Comparative Review of IPv4 and IPv6 for Research Test Bed [54]	Mohd.Kh airil ; Sailan ; Rosilah Hassan ; Ahmed Patel	2009	IPv4 , IPv6 , IPng , IPv6 Ready , Multi service router	Testing , Internet , Costs , Protocols , Informatics , Computer science , IP networks , Network address translation , Investments , Software measurement	Internet , intranets , IP networks	IPv6 network penetration , IPv4 address pool , research test bed product selection , Intranet , Regional Internet Registry	8	23
32	An Innovative Simulation, Comparison Methodology & Framework for evaluating the Performance of a	J. Hanumant happa ; D.H. Manjaiah ; C.V. Aravinda	2010	BD-SIIT , DSTM , IPv4 ,	Throughput , Protocols , Logic gates ,	computer network performance evaluation , Internet	performance evaluation , IPv4/IPv6 transition mechanism ,		14

	Novel IPv4/IPv6 Transition Mechanisms : BD-SIIT vs DSTM [55]			IPv6 , IPv4/IPv6 Address mapping etc	Tunneling , Internet Workstations , IP networks	, IP networks , protocols	BD-SIIT , DSTM , Internet , protocols , QoS control , encryption , decryption , mobility , routing , security , real time applications		
33	IPv4-v6 Configured Tunnel and 6to4 Transition Mechanisms Network Performance Evaluation on Linux Operating Systems [56]	Shaneel Narayan ; Sotharith Tauch	2010	IPv4 , IPv6 , transition mechanism , configured tunnel ,	Operating systems , Throughput , Jitter , Delay , Computers ,	computer network performance evaluation , data communication , Internet	IPv4 , IPv6 , 6to4 transition mechanisms , network performance evaluation	11	17

				6to4 , performance evaluation , Linux Fedora , Linux Ubuntu	Internet , Linux	, IP networks , Linux , transport protocols	, Linux operating systems , configured tunnel , data communications , Internet , ARPA , TCP , UDP		
34	An IPv6 Translation Scheme for Small and Medium Scale Deployment [57]	Yang Xia ; Bu Sung Lee ; Chai Kiat Yeo ; Vincent Lim Sok Seng	2010	IPv6 Transition , IPv6 Translation	Logic gates , Internet , Servers , Routing protocols , Linux , Multiplexing	Internet , IP networks , transport protocols	IPv6 translation scheme , small medium scale deployment , Internet , IPv4 address exhaustion , lightweight IPv4 IPv6 protocol translation scheme , GATE VI scheme	3	18

							, application layer gateway framework	
35	Providing Support for Legacy IPv4 Applications in IPv6 Network with Network Aware Mobility [58]	Markus Luoto ; Teemu Rautio ; Jukka Makela	2011		Mobile communication , Peer to peer computing , Throughput , Streaming media , Delay , Tunneling , Mobile computing	Internet , IP networks , mobility management (mobile radio)	legacy IPv4 application , IPv6 network , network aware mobility , transition mechanism , Internet , smartphones , tablets , netbooks , mobility management , tunneling based transition scheme , network aware mobile IPv6 testbed	23

36	IPv6 Tunnel Broker Implementation and Analysis for IPv6 and IPv4 Interconnection [59]	Aris Cahyadi Risdianto ; R. Rumani	2011	IPv4 , IPv6 , Dual IP Stack , Protocol Translation , Tunneling , IPv6 Tunnel Broker , FTP , ICMP	IP networks , Protocols , Tunneling , Degradation , Servers , Databases , Payloads	IP networks , transport protocols	IPv6 tunnel broker implementation , IPv6 interconnection ,IPv4 interconnection , TCP/IP protocol standard, Internet network growth , IP next generation , transition mechanisms, dual IP stack, protocol translation , dynamic tunneling mechanism , user request , network performance,IP header overhead, Linux operating system,FTP packet, ICMP packet		17
37	Transition from IPv4 to IPv6: A Translation Approach [60]	Yu Zhai ; Congxiao Bao ; Xing Li	2011	IVI , IPv4/IPv6 transition , IPv4/IPv6 translation ,	Multiplexing , IP networks , Internet , Protocols ,	Internet , IP networks , protocols , resource allocation	IPv4/IPv6 translation scheme , IANA , RIR , Internet ,	6	21

				IPv4/IPv6 coexistence	Heuristic algorithms , Logic gates , Routing		resource migration , protocol transition , IVI flavours		
38	The NAT64/DNS64 Tool Suite for IPv6 Transition [61]	Marcelo Bagnulo ; Alberto Garcia-Martinez ; Iljitsch Van Beijnum	2012		Filtering , Servers , Internet , Dual stacking , IP networks , Network address translation , Logic gates	Internet , IP networks	NAT64-DNS64 tool suite , IPv6 transition , Internet hosts , IPv4 address pool , IPv4 nodes , IPv6 nodes , dual stack , network address translation	6	15
39	4over6: Network Layer Virtualization for IPv4-IPv6 Coexistence [62]	Yong Cui ; Peng Wu ; Mingwei Xu ; Jianping Wu ; Yiu L. Lee ; Alain Durand ;	2012		Internet , Virtualization , IP networks ,	Internet , IP networks , next generation networks	network layer virtualization , IPv4-IPv6 coexistence , IPv4 address space ,	7	14

		Chris Metz			Next generation networking , Routing , Computer architecture , Network topology	, virtualisation	IPv6 transition technique , next generation Internet , dual stack segment , network infrastructure , 4over6 virtualization architecture , packet forwarding , ISP community , vendor community		
40	Tunnel-Based IPv6 Transition [63]	Yong Cui ; Jiang Dong ; Peng Wu ; Jianping Wu ; Chris Metz ; Yiu L. Lee ; Alain Durand	2013	IPv6 transition , next generation Internet , software , tunneling , 4over6	Tunneling , Internet , Encapsulation , IP networks , Routing , Protocols	Internet , IP networks	tunnel-based IPv6 transition , Internet community , like-to-unlike IP interconnectivity , like-to-like IP connectivity	4	15

					Payloads		access networks , transition problems		
41	An Investigation Into Teredo and 6to4 Transition Mechanisms: Traffic Analysis [64]	Martin Elich ; Petr Velan ; Tomas Jirsik ; Pavel Celeda	2013	Teredo , 6to4 , IPv6 , Transition Mechanisms	Protocols , Servers , Relays , Linux , Internet , IP networks , Geology	flow measureme nt , IP networks , network servers , telecommu nication traffic	teredo transition mechanism , 6to4 transition mechanism , IPv4 address , IPv6 transition mechanism , flow-based measurement system , IPv6 tunneled traffic analysis , Czech national research , education network , TTL , HOP limit distribution, Teredo server	4	16
42	Network Performance Evaluation of 6to4 and	Dinesh Hadiya ; Rohit Save ;	2013	Transition Mechanism ,	Internet , Operating systems	computer network performanc e evaluation	6to4 network performance evaluation ,		18

	Configured Tunnel Transition Mechanisms [65]	Geetu Geetu		Configured Tunnel , 6to4 , Network Performance , Windows Operating Systems	, Throughput , Protocols , Servers , IP networks , Delays	, Internet , IP networks , network operating systems	configured tunnel transition mechanisms , empirical test-bed analysis, IPv4 addresses , Internet protocol , IPv6 , Internet Engineering Task Force , IETF , network infrastructure , performance metrics ,throughput, jitter , delay , 6to4 transition mechanism , Windows operating systems		
43	Transition from IPv4 to IPv6: A State-of-the-Art Survey [66]	Peng Wu ; Yong Cui ; Jianping Wu ; Jiangchuan Liu ; Chris Metz	2013	IPv6 transition , heterogeneous network connectivity , translation , tunneling ,	Internet , Protocols , Routing , Tunneling , Scalability , IP networks , Security	computer network reliability , Internet , IP networks , tunnelling	IANA , Internet assigned numbers authority , global IPv4 address space , IPv6 transition process , availability , intercommunication ability , IETF , translation technique , tunneling technique ,	30	60

				heterogeneous addressing			practical network ISP		
44	Security Threats for IPv6 Transition Strategies: A Review [67]	Amjed Sid Ahmed ; Rosilah Hassan ; Nur Effendy Othman	2014	IPv4 , IPv6 , Dual Stack , Translation , Tunneling	Protocols , Tunneling , Internet , IP networks , Firewalls (computing) , Encapsulation	information systems , Internet , security of data , transport protocols	security threat , IPv6 transition strategy , protocol mechanism , IPv4 , classless addressing , NAT , information system , internet technology , cloud computing , mobile IP , IP-capable mobile telephony ,	3	12

							Internet engineering task force , IETF , dual stack , header translation , tunneling		
45	Study of packet level UDP performance of NAT44, NAT64 and IPv6 using iperf in the context of IPv6 migration [68]	Vitruvius John D. Barayuga ; William Emmanue l S. Yu	2014		Bandwidth , Jitter , Packet loss , Internet , Protocols , IP networks	bandwidth allocation , IP networks	IPv6 network , time transfer , iperf generic UDP mode , service providers , Philippines , computer networks , IPv4 network , network address translation , Internet Protocol version 6	5	18

							<ul style="list-style-type: none"> , RIR , Regional Internet Registries , IANA , Internet Assigned Number Authority , IPv6 migration , packet level UDP performance , NAT64 , NAT44 		
46	Performance Evaluation of IPv4/IPv6 Transition Mechanisms: IPv4-in-IPv6 Tunneling Techniques [69]	N. Chuangchunsong ; S. Kamolphiwong ; T. Kamolphiwong ; R. Elz ; P. Pongpaibool	2014	<ul style="list-style-type: none"> IPv6 , DS-Lite , 4over6 , 4rd , IPv4/IPv6 transition 	<ul style="list-style-type: none"> Delays , Ports (Computers) , Tunneling , Time factors , Routing , Reliability 	<ul style="list-style-type: none"> computer network reliability , delays , Internet , IP networks , quality of service 	<ul style="list-style-type: none"> IPv4-IPv6 transition mechanisms , IPv4-in-IPv6 tunneling techniques , IPv4 address space , Internet service providers , ISP 	2	10

					IP networks		<ul style="list-style-type: none"> , IPv4-IPv6 migration-transition tools , DS-lite , intracommunication reliability , quality-of-service , QoS , intercommunication reliability 		
47	Strategy and Study of the Transition Technologies from IPv4 to IPv6 [70]	Zhou Hong	2014	<ul style="list-style-type: none"> IPv6 , transitional technologies 	<ul style="list-style-type: none"> Tunneling , Lead 	<ul style="list-style-type: none"> Internet , IP networks , transport protocols 	<ul style="list-style-type: none"> transition technologies , IPv4 , IPv6 , Internet protocol , IPv6 , Internet technology 		9

48	A Survey of Transition Mechanisms from IPv4 to IPv6 – Simulated Test Bed and Analysis [71]	Saadullah Kalwar, Nafeesa Bohra, Aftab A. Memon	2015	IPv6 , transition strategies , NAT , dual stack , tunneling	Protocols , Internet , IP networks , Tunneling , Switches , Educational institutions , Standards	Internet , IP networks , protocols	IPv6 , IPv4 transition mechanism , protocol , defacto standard , Internet architecture , delay avoidance , IP address , Mehran University of Engineering and Technology , MUET , Jamshoro , Pakistan , GNS3 , Wireshark , DSTM	3	16
----	--	---	------	---	--	--	--	---	----

49	Performance Comparison Analysis of E2E Dual-Stack IP Protocol Method over Wired and Wi-Fi Broadband Acces [72]	Wan Mohd Nazmin Wan Mahmud ; Ruhani Ab Rahman ; Murizah Kassim ; Mat Ikram Yusof	2016	IPv6 , IPv4 , Dual-Stack , Round Trip Time , File Transfer Protocol , IPerf , Throughput , Response time	Broadband communication , IEEE 802.11 Standard , Internet Protocols , IP networks , Throughput , Time factors	Internet , transport protocols	E2E dual-stack IP protocol method , next-generation Internet protocol , IPv6 , IPv4 , Wi-Fi broadband access , Internet Service Provider , client-server test-bed , round trip time , file transfer protocol , Iperf test		12
50	Enhanced Security Architecture for IPv6 Transition [73]	D. Akilandes wari ; S. Albert Rabara ; T. Daisy	2017	tunneling , security , transition ,	Elliptic curve cryptography , Tunneling ,	data integrity , Internet ,	IPv6 transition , IPv4 addresses , transition techniques	1	13

		Premila Bai		elliptic curve cryptography	Computer architecture , Protocols , Internet	IP networks , public key cryptography	, tunneling mechanism , security attacks , enhanced security architecture , elliptic curve cryptography , ECC , IETF , data integrity		
51	Comparative Studies of IPv6 Tunnel Security [74]	Kejun Gu ; Liancheng Zhang ; Zhenxing Wang ; Yazhou Kong	2017	IPv6 , transition , tunnel , security , comparative studies	Security , Internet , Routing protocols , Servers , Relays , Manuals	computer network security , IP networks , transport protocols	IPv4 networks , IPv6 networks , tunnel mechanisms , security issues , security problems , IPv6 tunnel security , injection attack		17

							<ul style="list-style-type: none"> , address spoofing attack , reflector attack , security countermeasures , deep packet inspection , IPsec 		
52	When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks [75]	Hyunwook Hong ; Hyunwoo Choi ; Dongkwann Kim ; Hongil Kim ; Byeongdo Hong ; Jiseong Noh ; Yongdae Kim	2017	Cellular Network <ul style="list-style-type: none"> , Middlebox , IPv6 	Cellular networks <ul style="list-style-type: none"> , Middleboxes , IP networks , Mobile handsets , Security , Logic gates 	cellular radio <ul style="list-style-type: none"> , firewalls , IP networks , telecommunication services 	IPv6 cellular networks , middlebox security problems , cellular operators , IP address , cellular middleboxes , stateful NAT64 boxes , backward compatibility, IPv4 services, IPv6 middlebox , firewalls, cellular devices ,	2	43

							denial-of-service attacks , over-billing attacks , IPv6 address , IPv4 address , NAT overflow attack , NAT resources , NAT wiping attack , active NAT mappings , TCP sequence number verification , NAT bricking attack , IP-based blacklisting		
53	Estimating of the preparedness level of telecommunications operators for the introduction of IPv6 in the own networks [76]	Vadym Kaptur ; Andrey Kviatkovsky	2017	IPv4 , IPv6 , migration , dual stack , tunneling	Protocols , Internet , Hardware , Software , Government , Tunneling	IP networks , transport protocols	telecommunication companies , telecommunications operators , comparative analysis , telecommunication networks , IP protocol , tunneling , encapsulation , IPv6 stack , translation technology, IPv4 ,		7

							IPv6 telecommunications networks , modified analytic hierarchy process , IP		
54	Implementation and Testing of IPv6 Transition Mechanisms [77]	Jesus Marco Vivas Ruiz ; Carlos Silva Cardenas ; Jose Luis Muñoz Tapia	2017	IPv6 , transition mechanisms , virtualization , hybrid network addressing	Linux , Tools , Virtualization , Protocols , Network topology , Tunneling , Relays	IP networks , telecommunication network topology	topologies , translation mechanisms , DNS64 , NAT64 , DHCPv6 , IPv6 transition mechanisms , virtual lab , IPv6 networks		20
55	Transition from IPv4 to IPv6 in Bangladesh: The Competent and Enhanced Way to Follow [78]	Fatema Siddika ; Md. Anwar Hossen ; Sajeeb Saha	2017	IPv6 , IPv6 Transition , IPv6 Deployment , IPv6 performance , IPv6 in Bangladesh ,	Internet , Protocols , Network topology , Tunneling , IP networks , Throughput , Topology	computer network security , IP networks	IPv4 to IPv6 transition , Bangladesh , ISP , security vulnerability , IPv6 deployment , dual stack transition	1	17

				Dual-Stack , 6to4 Tunnel			, tunneling technique		
56	Analysis of Organizations IPv6 Deployment Strategies in Nigeria and Evaluating Suitable Transition Mechanisms [79]	Mohammed F. Suleiman ; Julien Cordry	2017	ipv6 , ipv4 , dual-stack ,6to4 tunneling , internet , ip address , NAT , transition mechanism , network	Protocols , Internet , IP networks , Companies , Government	Internet , IP networks , protocols	IPv4 , IPv6 adoption , Next generation Internet Protocol ,Internet communication protocol , IPv6 deployment strategies		40
57	Performance Analysis of Native Ipv4/Ipv6 Networks Compared to 6to4 Tunnelling Mechanism [80]	Mohammed S. Ali ; Tara A. Yahiya	2018	IPv4 , IPv6 , 6to4 , Tunnel ling	Delays , Tunneling , IP networks , Internet , Workstations , Time factors , Protocols	IP networks	6to4 tunnelling mechanism , Ipv4/Ipv6 networks , tunnelling transition technique , dual-stack mechanism , translation mechanism ,		7

							tunneling mechanism		
58	Evaluation of IPv6 transition mechanisms using QoS service policies [81]	Luke Smith ; Mark Jacobi ; Samir Al-Khayatt	2018	IPv4 , IPv6 , QoS , NAT64 , 6to4 tunneling , Cisco , IXIA	Quality of service , Tunneling , Topology , Network topology , Bandwidth , Manuals , Generators	IP networks , quality of service , telecommunication traffic	IPv6 network , providers core data networks , IPv6 traffic transitions , core IPv4 network traffic generators , data capture tools , IPv6 transition mechanisms , QoS service policies , service policies , quality of service , Cisco ISR 4351		13
59	Migrating from IPV4 to IPV6 in Jamaica [82]	Christopher Udeagha ; R. Martin ; D. Peck ;	2018	IP , IPV4 ,	Protocols , IP networks ,	IP networks ,	IPv4 addresses , Jamaica , Internet protocol version 4 ,		13

		A. Youton ; A. Marshall ; J. Clarke		IPV6 , migrating , technology , local industries	Routing , Internet , Security , Tunneling , Industries	telecommu nication network routing	Internet protocol version 6 , IPv6 , packet processing , improved IP securities , green technique , word length 128.0 bit , size 6.0 inch		
--	--	-------------------------------------	--	--	--	------------------------------------	---	--	--

Fuente: Elaboración propia

Resultados

1.- ¿Existe alguna otra solución haciendo uso del mecanismo de tunelización?

De los 59 artículos hay 4 que proponen nuevas soluciones basándose en el mecanismo de tunelización, ya que ellos realizaron modificaciones en la forma que se implementa la tunelización debido a que en la situación en la que se encontraban los autores la tunelización servía para algunas secciones de la red y no cubría toda la infraestructura.

TABLA XI SOLUCIONES BASANDOSE EN TUNELIZACIÓN

Nº	Artículo	Autores	Solución
1	[8]	Kai Wang, Ann-Kian Yeo, A. L. Ananda	TDT(Solución de Transición de túnel dinámico)
2	[23]	Shiang-Ming Huang ; Quincy Wu ; Yi-Bing Lin	SymTeredo
3	[48]	Ra'ed AlJa'afreh ; John Mellor ; Mumtaz Kamala ; Basil Kasasbeh	Sistema de mapeo bidireccional (BDMS)
4	[50]	Hailin An ; Wanming Luo ; Xingfeng Li ; Xinchang Zhang ; Baoping Yan	Túnel IPv6-in-IPv4-UDP llamado Escort,

Kai Wang, Ann-Kian Yeo, A. L. Ananda propuso una solución transparente y escalable llamada TDT(Solución de Transición de túnel dinámico) basada en las técnicas de tunelización dinámico y Dual Stack. Las fases de esta solución son las siguientes: Primero se solicita direcciones IPv4 para luego asignarlas dinámicamente. Segundo, cada dispositivo que está en la red IPv6 tiene que estar actualizado para que soporte direcciones IPv6. Seguido se configura todos los hosts como clientes TDT, además se implementa los servidores AAS con direcciones IPv4 dentro de la subred. Después una red IPv4 se convertirá en una subred IPv6. Al finalizar la implementación de esta solución se observó que se pudo alcanzar los nodos que hacían uso de Dual Stack con los otros nodos que utilizaban túnel dinámico.

Shiang-Ming Huang, Quincy Wu, y Yi-Bing Lin explica que el Túnel Teredo no funciona con NAT simétrico. Por lo tanto, propone SymTeredo, una extensión de Teredo que solucionaría el problema que tiene este mecanismo de transición. Para implementar esta nueva técnica se realiza lo siguiente: El cliente SymTeredo establece el formato de dirección IPv6 cuando se detecta que el NAT es simétrico. Este procedimiento se ejecuta antes de la entrega de paquetes cuando se establece el indicador simétrico en la dirección IPv6 de destino. El relé SymTeredo determina el destino UDP de IPv4 de un paquete encapsulado de acuerdo con la asignación correspondiente almacenado en la caché de direcciones cuando se establece el indicador simétrico en la dirección IPv6 de destino. La omisión de esta comprobación puede traer amenazas de seguridad adicionales para el relé de SymTeredo.

2.- ¿Se muestran etapas claras para realizar la migración de IPv4 a IPv6?

De los 59 artículos hay 13 que proponen etapas para realizar la migración gradual. Esto es importante debido a que da una idea amplia para elegir que etapa se podría implementar al migrar a IPv6.

TABLA XII ARTÍCULOS QUE PLANTEAN ETAPAS DE MIGRACIÓN

Nº	Artículo	Autores	Título del artículo
1	[11]	Juha Wiljakka, Nokia	Transition to IPv6 in GPRS and WCDMA Mobile Networks
2	[14]	Mallik Tatipamula ,Patrick Grossetete, Hiroshi Esaki	IPv6 Integration and Coexistence Strategies for Next-Generation Networks
3	[19]	Ed Jankiewicz ; Kwai Fung Chan ; David Green	AN APPROACH TO IPV6 TRANSITION IN WIRELESS NETWORKS
4	[20]	Georgios Koutepas ; Athanasios Douitsis ; Demetris Philippides ; Vasilis Maglaris	An Approach for the Administration and Security of IPv6 Transition Mechanisms: An SNMP MIB for 6to4
5	[21]	S. McFarland	IPv6 Solutions for NAT Overlap
6	[44]	Tricia Dunn	The IPv6 Transition
7	[46]	Wenming Shi ; Chuanhe Huang ; Qinggang Wang ; Yan Chen ; Yiming Huang ; Yong Cheng	A Novel IPv4/IPv6 Translation Mechanism Based on NAT-PT
8	[52]	Asif Nawaz ; Mahmood Ashraf ; X. B. Hong ; J. Wu ; J. T. Lin	IPv4 to IPv6 Evolution Strategies of Pakistan Internet Exchang
9	[54]	Mohd.Khairil Sailan ; Rosilah Hassan ; Ahmed Patel	A Comparative Review of IPv4 and IPv6 for Research Test Bed
10	[60]	Yu Zhai ; Congxiao Bao ; Xing Li	Transition from IPv4 to IPv6: A Translation Approach
11	[66]	Peng Wu ; Yong Cui ; Jianping Wu ; Jiangchuan Liu ; Chris Metz	Transition from IPv4 to IPv6: A State-of-the-Art Survey
12	[69]	N. Chuangchunsong ; S. Kamolphiwong ; T. Kamolphiwong ; R. Elz ; P. Pongpaibool	Performance Evaluation of IPv4/IPv6 Transition Mechanisms: IPv4-in-IPv6 Tunneling Techniques
13	[78]	Fatema Siddika ; Md. Anwar Hossen ; Sajeeb Saha	Transition from IPv4 to IPv6 in Bangladesh: The Competent and Enhanced Way to Follow

3.- ¿Qué tipo de seguridad se podrían implementar en los mecanismos de transición?

De los 59 artículos hay 10 que implementan seguridad en los mecanismos de transición para mitigar algunos riesgos que se podrían ocasionar en la red.

TABLA XIII ARTÍCULOS QUE PROPONEN TIPOS DE SEGURIDAD

N°	Artículo	TITULO	SEGURIDAD
1	[19]	AN APPROACH TO IPV6 TRANSITION IN WIRELESS NETWORKS	IPSEC
2	[20]	An Approach for the Administration and Security of IPv6 Transition Mechanisms: An SNMP MIB for 6to4	Lista de control de acceso (ACL)
3	[47]	Security Mechanisms for the IPv4 to IPv6 Transition	Modelo híbrido: Firewall y Sistema de detección de intrusos (IDS)
4	[51]	IPv6 Security Challenges	Secure Neighbor Discovery, IPSEC, Firewall
5	[53]	An Overview of IPv4 to IPv6 Transition and Security Issues	Firewall, IDS, Sistema de prevención de intrusos (IPS)
6	[54]	A Comparative Review of IPv4 and IPv6 for Research Test Bed	IPSEC
7	[59]	IPv6 Tunnel Broker Implementation and Analysis for IPv6 and IPv4 Interconnection	Secure Sockets Layer(SSL)
8	[65]	Network Performance Evaluation of 6to4 and Configured Tunnel Transition Mechanisms	IPSEC
9	[67]	Security Threats for IPv6 Transition Strategies: A Review	Lista de control de acceso (ACL)
10	[70]	Strategy and Study of the Transition Technologies from IPv4 to IPv6	Application Layer Gateway(ALG)

Luego que se recopiló los artículos se agruparon por el tipo de seguridad para saber cual es el que implementan mayormente.

TABLA XIV AGRUPACIÓN POR TIPO DE SEGURIDAD

N°	SEGURIDAD	CANTIDAD
1	IPSEC	4
2	Firewall	3
3	ACL	2
4	IDS	2
5	IPS	1
6	ALG	1
7	SSL	1
8	Secure Neighbor Discovery	1

Como se puede observar el tipo de seguridad que se utiliza mayormente es IPSEC debido a que es un protocolo que ya viene integrado en los Protocolos de Internet. En segundo lugar, se encuentra el Firewall que ayudaría bloquear los accesos no autorizados a la red.

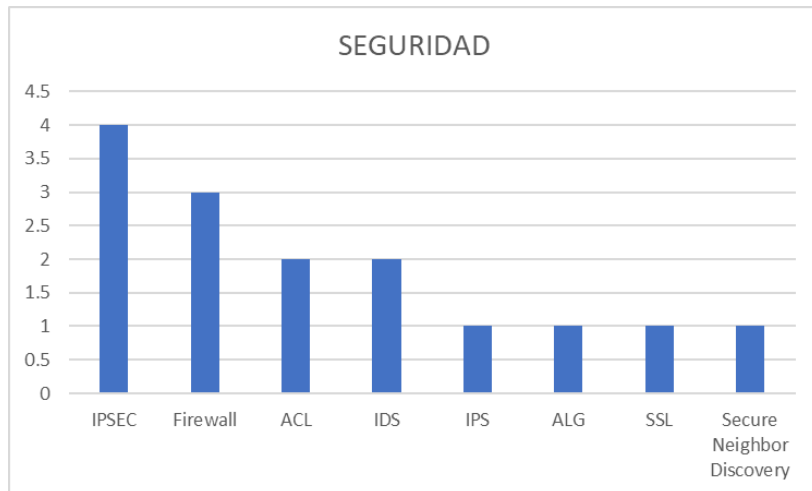


Fig. 25 Tipos de Seguridad para los mecanismos de transición

Fuente: Elaboración propia

4.- ¿Qué mecanismos de transición se implementaron?

De los 59 artículos hay 30 que implementan mecanismos de transición para luego evaluarlos según las métricas que cada autor ha seleccionado.

TABLA XV ARTÍCULOS QUE IMPLEMENTAN MECANISMOS DE TRANSICIÓN

Nº	Artículo	AUTORES	Mecanismo
1	[10]	M. Samad, F.Yusuf, Habibah Hashim y Md Mahhdz Md Zan	Tunelización, Dual Stack
2	[11]	Juha Wiljakka, Nokia	Traducción
3	[12]	Eun-Young Park, Jae-Hwoon Lee ; Eun-Young Park, Jae-Hwoon Lee	Dual Stack
4	[13]	Jiann-Liang Chen, Yao-Chung Chang y Chien-Hsiu Lin	Tunelización
5	[18]	H.M. Tahir ; A. Taa ; N.B.M. Nasir	Dual Stack
6	[19]	Ed Jankiewicz ; Kwai Fung Chan ; David Green	Traducción
7	[20]	Georgios Koutepas ; Athanasios Douitsis ; Demetris Philippides ; Vasilis Maglaris	Tunelización
8	[21]	S. McFarland	Traducción
9	[24]	S. Tomic ; T. Hoehner ; R. Menedetter ; R. Maslenka ; M. Banfield ; R. Lauster	Traducción, Tunelización
10	[45]	Mohamed Boucadair ; Yoann NOISETTE	Traducción
11	[26]	Min Ho Park ; Jung Tae Kim ; Eui Hyun Paik	Dual Stack, Traducción, Tunelización
12	[46]	Wenming Shi ; Chuanhe Huang ; Qinggang Wang ; Yan Chen ; Yiming Huang ; Yong Cheng	Traducción
13	[47]	Abidah Hj Mat Taib ; Rahmat Budiarto	Dual Stack
14	[49]	Shaneel Narayan ; Samad S. Kolahi ; Yonathan Sunarto ; Du D. T. Nguyen ; Paul Man	Dual Stack

15	[50]	Hailin An ; Wanming Luo ; Xingfeng Li ; Xinchang Zhang ; Baoping Yan	Tunelización
16	[55]	J. Hanumanthappa ; D.H. Manjaiah ; C.V. Aravinda	Dual Stack
17	[56]	Shaneel Narayan ; Sotharith Tauch	Tunelización
18	[58]	Markus Luoto ; Teemu Rautio ; Jukka Makela	Tunelización
19	[59]	Aris Cahyadi Risdianto ; R. Rumani	Tunelización
20	[60]	Yu Zhai ; Congxiao Bao ; Xing Li	Traducción
21	[61]	Marcelo Bagnulo ; Alberto Garcia-Martinez ; Iljitsch Van Beijnum	Traducción
22	[62]	Yong Cui ; Peng Wu ; Mingwei Xu ; Jianping Wu ; Yiu L. Lee ; Alain Durand ; Chris Metz	Tunelización
23	[63]	Yong Cui ; Jiang Dong ; Peng Wu ; Jianping Wu ; Chris Metz ; Yiu L. Lee ; Alain Durand	Tunelización
24	[64]	Martin Elich ; Petr Velan ; Tomas Jirsik ; Pavel Celeda	Tunelización
25	[65]	Dinesh Hadiya ; Rohit Save ; Geetu Geetu	Tunelización
26	[66]	Peng Wu ; Yong Cui ; Jianping Wu ; Jiangchuan Liu ; Chris Metz	Traducción, Tunelización
27	[68]	Vitruvius John D. Barayuga ; William Emmanuel S. Yu	Traducción
28	[69]	N. Chuangchunsong ; S. Kamolphiwong ; T. Kamolphiwong ; R. Elz ; P. Pongpaibool	Tunelización
29	[71]	Saadullah Kalwar, Nafeesa Bohra, Aftab A. Memon	Traducción
30	[72]	Wan Mohd Nazmin Wan Mahmud ; Ruhani Ab Rahman ; Murizah Kassim ; Mat Ikram Yusof	Dual Stack

Luego que se recopiló los artículos se agruparon por el tipo de mecanismo para saber cuál es el que implementó mayormente.

TABLA XVI AGRUPACIÓN POR TIPO DE MECANISMO DE TRANSICIÓN

Nº	MECANISMOS	CANTIDAD
1	Dual Stack	8
2	Tunelización	15
3	Traducción	12

Según los artículos de la tabla XV el tipo de mecanismo más implementado es la Tunelización.

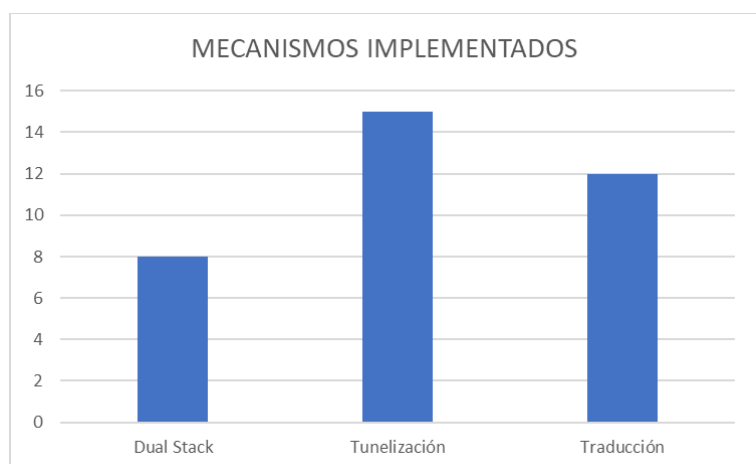


Fig. 26 Cantidad de veces que se utilizó cada mecanismo de transición

Fuente: Elaboración propia

Conclusiones

El motivo principal para realizar esta migración es debido al agotamiento de direcciones IPv4, por lo tanto, las empresas que brindan algún tipo de servicio a sus clientes deberían realizar la implementación de los mecanismos de transición ya que es una manera gradual de realizar la migración de una red Ipv4 a una red IPv6 por lo tanto se basó en una revisión sistemática respecto a los mecanismos de transición para responder a las interrogantes planteadas anteriormente lo cual permitió identificar los artículos que brindaron solución a las preguntas respecto a las etapas de la migración, el tipo de seguridad que se podría implementar y sobre todo saber que otras soluciones se están planteando mejorando los mecanismos.

Bibliografía

[Gerencia, «Adiós IPv4, bienvenido IPv6,» *Gerencia*, Julio 2014.

1

]

[Lacnic, «Lacnic,» 04 Noviembre 2018. [En línea]. Available:

2 <http://www.lacnic.net/web/lacnic/agotamiento-ipv4>.

]

[Lacnic, «Lacnic,» s.f. [En línea]. Available: <http://www.lacnic.net/despliegaIPv6>.

3

]

[Google, «Estadísticas,» 02 Noviembre 2018. [En línea]. Available:

4 <https://www.google.com/intl/es/ipv6/statistics.html#tab=ipv6-adoption>.

]

[A. Gomez, «Reporte Digital,» 19 Septiembre 2016. [En línea]. Available:

5 <https://reportedigital.com/transformacion-digital/adoptar-ipv6-grandes-empresas/>.

]

[IPv6 Mx, «IPv6 Mx,» s.f. [En línea]. Available:

6 <http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/106->

7 [enterprisenotreadyipv6](http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/106-enterprisenotreadyipv6).

]

[«IPv6 portal,» s.f. [En línea]. Available: <http://portalipv6.lacnic.net/como-es-la->

7 [transicion/](http://portalipv6.lacnic.net/como-es-la-transicion/).

]

[K. Wang, A. Yeo y A. Ananda, «DTTS: a transparent and scalable solution for IPv4 to IPv6 transition,» *IEEE*, 2001.

8

]

[A. Durand, «Deploying IPv6,» *IEEE*, 2001.

9

]

[M. Samad, F. Yusuf, H. Hashim, M. Mahfudz y M. Zan, «Deploying Internet Protocol version 6 (IPv6) over Internet Protocol version 4 (IPv4) tunnel,» *IEEE*, 2002.

]

[J. Wiljakka, «Transition to IPv6 in GPRS and WCDMA mobile networks,» *IEEE*, pp. 134 - 140, 2002.

1

]

[E.-Y. Park, J.-H. Lee y B.-G. Choe, «An IPv4-to-IPv6 dual stack transition mechanism supporting transparent connections between IPv6 hosts and IPv4 hosts in integrated IPv6/IPv4 network,» *IEEE*, 2004.

]

[J.-L. Chen, Y.-C. Chang y C.-H. Lin, «Performance investigation of IPv4/IPv6 transition mechanisms,» *IEEE*, 2004.

3

]

[M. Tatipamula, P. Grossetete y H. Esaki, «IPv6 integration and coexistence strategies for next-generation networks,» *IEEE*, 2004 .

4

]

[I.-P. Hsieh y S.-J. Kao, «Managing the Co-existing Network of IPv6 and IPv4 under Various,» *IEEE*, 2005.

5

]

[T. Camilo y S. pasqualini, «A Global Perspective of IPv6 Native and,» *IEEE*, 2006.

1

6

]

[S. Hong, N. Ko, H. Ryu y N. Kim, «New IPv6 Transition Mechanism based on End-to-End Tunnel,» *IEEE*, 2006.

7

]

[H. Tahir, A. Taa y N. Nasir, «Implementation of IPv4 Over IPv6 using Dual Stack Transition Mechanism (DSTM) on 6iNet,» *IEEE*, 2006.

8

]

[E. Jankiewicz, K. F. Chan y D. Green, «An Approach to IPv6 Transition in Wireless
1 Networks,» *IEEE*, 2007.

9

]

[G. Koutepas, A. Douitsis y D. Philippid, «An Approach for the Administration and
2 Security of IPv6 Transition Mechanisms: An SNMP MIB for 6to4,» *IEEE*, 2006.

0

]

[S. McFarland, «IPv6 Solutions for NAT Overlap,» *IEEE*, 2006.

2

1

]

[M.-K. Shin, H.-J. Kim, D. Santay y D. Montgomery, «An empirical analysis of IPv6
2 transition mechanisms,» *IEEE*, 2006.

2

]

[S.-M. Huang, Q. Wu y Y.-B. Lin, «Enhancing Teredo IPv6 tunneling to traverse the
2 symmetric NAT,» *IEEE*, 2006.

3

]

[S. Tomic, T. Hoehner, R. Menedetter, R. Maslenka y M. Banfi, «Study of SIP-based
2 VoIP Application Interworking with IPv4-IPv6 Transitioning Mechanisms,» *IEEE* ,
4 2006.

]

[T. Hoehner, M. petraschek, S. Tomic y M. Hirsch, «Performance Evaluation of SIPv6
2 Transitioning,» *IEEE*, 2007.

5

]

[M. H. Park, J. T. Kim y E. H. Paik, «Deployment Strategy And Performance
2 Evaluation of The IPv6 Home Network Using The Home Server,» *IEEE*, 2007.

6

]

[E. Bellido Quintero, Equipos de interconexión y servicios de red (UF1879),
2 Antequera: IC Editorial, 2014.

7

]

[G. Benites, «Conversión de una dirección binaria a decimal y Conversión de decimal
2 en binario - CCNA1 V5 - CISCO C8,» 27 Julio 2017. [En línea]. Available:

8 <http://www.ingenieriasystems.com/2017/07/conversion-de-una-direccion-binaria->

] [decimal-conversion-decimal-binario-ccna1v5-cisco-c8.html](http://www.ingenieriasystems.com/2017/07/conversion-de-una-direccion-binaria-decimal-conversion-decimal-binario-ccna1v5-cisco-c8.html).

[J. Dariene , Método para la transición a IPv6 en los proveedores de servicios privados
2 de Cuba, La Habana: D - Instituto Superior Politécnico José Antonio Echeverría.
9 CUJAE, 2011.

]

[A. Aznar López, La red Internet. El modelo TCP/IP, Madrid: Grupo Abantos
3 Formación y Consultoría, 2005.

0

]

[I. Martínez y P. Riaño, IPv6-Lab: entorno de laboratorio para la adquisición de
3 competencias relacionadas con IPv6, Alcalá de Henares: UNIVERSIDAD DE
1 ALCALA DE HENARES , 2015.

]

[R. J. Castaño Ribes y J. López Fernández, Redes locales, Madrid: Macmillan Iberia,
3 S.A. , 2013.

2

]

[F. Boronat Seguí y M. Montagud Climent, Direccionamiento e interconexión de
3 redes basada en TCP/IP, Valencia: Editorial de la Universidad Politécnica de
3 Valencia, 2013.

]

[F. Sepulveda, «Topología de Stack Doble IPv4/IPv6,» 03 Agosto 2011. [En línea].
3 Available: <https://es.slideshare.net/bramstoker/stack-doble-ipv4ipv6>.

4

]

[L. A. Canela, «Mecanismos de transición de IPv4 a IPv6,» 10 Octubre 2016. [En
3 línea]. Available: [https://community.cisco.com/t5/discusiones-routing-y-
5 switching/mecanismos-de-transicion-de-ipv4-a-ipv6/td-p/2986009](https://community.cisco.com/t5/discusiones-routing-y-switching/mecanismos-de-transicion-de-ipv4-a-ipv6/td-p/2986009).

]

[S. Narayanan, «Performance Analysis of 4to6 and 6to4 Transition Mechanisms over
3 Point to Point and IPsec VPN Protocols,» *IEEE*, 02 Febrero 2016.

6

]

[CISCO, «IPv6 Rapid Deployment,» s.f. [En línea]. Available:

3 [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&
7 uact=8&ved=2ahUKEwjnnNj76NLeAhWFylkKHV5WA98QFjACegQIBxAC&url=
\] \[https%3A%2F%2Fwww.cisco.com%2F%2Fen%2Fus%2Ftd%2Fdocs%2Fios-
xml%2Fios%2Finterface%2Fconfiguration%2Fxe-3s%2Ffir-xe-3s-book%2F\]\(https://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/fir-xe-3s-book\).](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwjnnNj76NLeAhWFylkKHV5WA98QFjACegQIBxAC&url=https%3A%2F%2Fwww.cisco.com%2F%2Fen%2Fus%2Ftd%2Fdocs%2Fios-xml%2Fios%2Finterface%2Fconfiguration%2Fxe-3s%2Ffir-xe-3s-book%2F)

[L. Koršič y M. Straus Istenič, «IPv4/IPv6 Transition Mechanisms,» s.f. [En línea].
3 Available:

[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&
uact=8&ved=2ahUKEwi_sIyi88_eAhUFmVkkHbIsA48QFjAAegQICBAC&url=htt](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi_sIyi88_eAhUFmVkkHbIsA48QFjAAegQICBAC&url=htt)

8 p%3A%2F%2Fmeetings.ripe.net%2Fdubrovnik2011%2Ffiles%2FIPv6_Transition_]
] Mechanisms_Ripe_07092011_v1.2.pdf&usg=AOvVaw1L0wb.

[CISCO, «Manually Configured IPv6 over IPv4 Tunnels,» s.f. [En línea]. Available:
3 [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwib86W47M_eAhUBr1kKHXzUAp4QFjAAegQICBAC&url)
9 [uact=8&ved=2ahUKEwib86W47M_eAhUBr1kKHXzUAp4QFjAAegQICBAC&url](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwib86W47M_eAhUBr1kKHXzUAp4QFjAAegQICBAC&url)
] =[https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fios-](https://www.cisco.com/fen/fus/ftd/docs/fios-xml/fios/interface/configuration/xe-3s/fir-xe-3s-book/)
xml%2Fios%2Finterface%2Fconfiguration%2Fxe-3s%2Ffir-xe-3s-book%.

[P. Colomé, «Implementando NAT en routers Cisco,» 18 Agosto 2010. [En línea].
4 Available: [http://www.redescisco.net/sitio/2010/08/18/implementando-nat-en-](http://www.redescisco.net/sitio/2010/08/18/implementando-nat-en-0-routers-cisco/)
0 routers-cisco/.

]

[J. D. a. P. A. Laplante, «Integrative Literature Review Review and Analysis of
4 Software Development Team Communication Research,» *IEEE*, 2017.

1

]

[Scimago Journal & Country Rank,
4 «[https://www.scimagojr.com/journalrank.php?area=1700&category=1705,](https://www.scimagojr.com/journalrank.php?area=1700&category=1705)» [En
2 línea].

]

[V. Casey, «Developing trust in virtual software development teams,» *Journal of*
4 *Theoretical and Applied Electronic Commerce Research*, 2010.

3

]

[T. Dunn, «The IPv6 Transition,» *IEEE*, 2002.

4

4

]

[M. Boucadair, M. Boucadair, M. Boucadair y M. Boucadair, «Migrating SIP-based
4 Conversational Services to IPv6,» *IEEE*, 2007.

5

]

[W. Shi, C. Huang, Q. Wang, Y. Chen, Y. Huang y Y. Cheng, «A Novel IPv4/IPv6
4 Translation Mechanism Based on NAT-PT,» *IEEE*, 2007.

6

]

[A. H. M. Taib y R. Budiarto, «Security Mechanisms for the IPv4 to IPv6 Transition,»
4 *IEEE*.

7

]

[R. AlJa'afreh, J. Mellor, M. Kamala y B. Kasasbeh, «Bi-Directional Mapping System 4 as a New IPv4/IPv6 Translation Mechanism,» *IEEE*, 2008.

8

]

[S. Narayan, S. S. Kolahi, Y. Sunarto, D. D. T. Nguyen y P. Man, «Performance 4 Comparison of IPv4 and IPv6 on Various Windows Operating Systems,» *IEEE*, 9 2008.

]

[H. An, W. Luo, X. Li, X. Zhang y B. Yan, «A new IPv6 Tunneling Protocol:Escort,» 5 *IEEE*, 2009.

0

]

[C. E. Caicedo, J. B. Joshi y S. R. Tuladhar, «IPv6 Security Challenges,» *IEEE*, 2009.

5

1

]

[A. Nawaz, M. Ashraf, X. B. Hong, J. Wu y J. T. Lin, «IPv4 to IPv6 Evolution 5 Strategies of Pakistan Internet Exchang,» *IEEE*, 2019.

2

]

[M. R. Sabir, M. A. Fahiem y M. S. Mian, «An Overview of IPv4 to IPv6 Transition 5 and Security Issues,» *IEEE*, 2009.

3

]

[M. Sailan, R. Hassan y A. Patel, «A Comparative Review of IPv4 and IPv6 for 5 Research Test Bed,» *IEEE*, 2009.

4

]

[J. Hanumanthappa, D. Manjaiah y C. Aravinda, «An Innovative 5 Simulation, Comparison Methodology & Framework for evaluating the Performance 5 evaluation of a Novel IPv4/IPv6 Transition Mechanisms : BD-SIIT vs DSTM,»] *IEEE*, 2010.

[S. Narayan y S. Tauch, «IPv4-v6 Configured Tunnel and 6to4 Transition 5 Mechanisms Network Performance Evaluation on Linux Operating Systems,» *IEEE*,

6 2010.

]

[Y. Xia, B. S. Lee, C. K. Yeo y V. L. S. Seng, «An IPv6 Translation Scheme for 5 Small and Medium Scale Deployment,» *IEEE*, 2010.

7

]

[M. Luoto, T. Rautio y J. Makela, «Providing Support for Legacy IPv4 Applications
5 in IPv6 Network with Network Aware Mobility,» *IEEE*, 2011.

8

]

[A. C. Risdianto y R. Ruman, «IPv6 Tunnel Broker Implementation and Analysis for
5 IPv6 and IPv4 Interconnection,» *IEEE*, 2011.

9

]

[Y. Zhai, C. Bao y X. Li, «Transition from IPv4 to IPv6: A Translation Approach,»
6 *IEEE*, 2011.

0

]

[M. Bagnulo, A. Garcia-Martinez y I. V. Beijnum, «The NAT64/DNS64 Tool Suite
6 for IPv6 Transition,» *IEEE*, 2012.

1

]

[Y. Cui, P. Wu, M. Xu, J. Wu, Y. L. Lee, A. Durand y C. Metz, «4over6: Network
6 Layer Virtualization for IPv4-IPv6 Coexistence,» *IEEE*, 2012.

2

]

[Y. Cui, J. Dong, P. Wu, J. Wu, C. Metz, Y. L. Lee y A. Durand, «Tunnel-Based IPv6
6 Transition,» *IEEE*, 2013.

3

]

[M. Elich, P. Velan, T. Jirsik y P. Celeda, «An Investigation Into Teredo and 6to4
6 Transition Mechanisms: Traffic Analysis,» *IEEE*, 2013.

4

]

[D. Hadiya, R. Save y G. Geetu, «Network Performance Evaluation of 6to4 and
6 Configured Tunnel Transition Mechanisms,» *IEEE*, 2013.

5

]

[P. Wu, Y. Cui, J. Wu, J. Liu y C. Metz, «Transition from IPv4 to IPv6: A State-of-
6 the-Art Survey,» *IEEE*, 2013.

6

]

[A. S. Ahmed, R. Hassan y N. E. Othman, «Security Threats for IPv6 Transition
6 Strategies: A Review,» *IEEE*, 2014.

7

]

[V. J. D. Barayuga y W. E. S. Yu, «Study of packet level UDP performance of
6 NAT44, NAT64 and IPv6 using iperf in the context of IPv6 migration,» *IEEE*, 2014.
8
]

[N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong, R. Elz y P. Pongpaibool,
6 «Performance Evaluation of IPv4/IPv6 Transition Mechanisms: IPv4-in-IPv6
9 Tunneling Techniques,» *IEEE*, 2014.
]

[Z. Hong, «Strategy and Study of the Transition Technologies from IPv4 to IPv6,»
7 *IEEE*, 2014.
0
]

[N. B. A. A. M. Saadullah Kalwar, «A Survey of Transition Mechanisms from IPv4 to
7 IPv6 – Simulated Test Bed and Analysis,» *IEEE*, 2015.
1
]

[W. M. N. W. Mahmud, R. A. Rahman, M. Kassim y M. I. Yusof, «Performance
7 Comparison Analysis of E2E Dual- Stack IP Protocol Method over Wired and Wi-Fi
2 Broadband Acces,» *IEEE*, 2016.
]

[D. Akilandeswari, S. A. Rabara y T. D. P. Bai, «Enhanced Security Architecture for
7 IPv6 Transition,» *IEEE*, 2017.
3
]

[K. Gu, L. Zhang, Z. Wang y Y. Kong, «Comparative Studies of IPv6 Tunnel
7 Security,» *IEEE*, 2017.
4
]

[H. Hong, H. Choi, D. Kim, H. Kim, B. Hong, J. Noh y Y. Kim, «When Cellular
7 Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks,»
5 *IEEE*, 2017.
]

[V. Kaptur y A. Kviatkovsky, «Estimating of the preparedness level of
7 telecommunications operators for the introduction of IPv6 in the own networks,»
6 *IEEE*, 2017.
]

[J. M. V. Ruiz, C. S. Cardenas y J. L. M. Tapia, «Implementation and Testing of IPv6
7 Transition Mechanisms,» *IEEE*, 2017.
7
]

[F. Siddika, M. A. Hossen y S. Saha, «Transition from IPv4 to IPv6 in Bangladesh: 7 The Competent and Enhanced Way to Follow,» *IEEE*, 2017.

8

]

[M. F. Suleiman y J. Cordry, «Analysis of Organizations IPv6 Deployment Strategies 7 in Nigeria and Evaluating Suitable Transition Mechanisms,» *IEEE*, 2017.

9

]

[M. S. Ali y T. A. Yahiya, «Performance Analysis of Native Ipv4/Ipv6 Networks 8 Compared to 6to4 Tunnelling Mechanism,» *IEEE*, 2018.

0

]

[L. Smith, M. Jacobi y S. Al-Khayatt, «Evaluation of IPv6 transition mechanisms 8 using QoS service policies,» *IEEE*, 2018.

1

]

[C. Udeagha, R. Martin, D. Peck, A. Youton, A. Marshall y J. Clarke, «Migrating 8 from IPV4 to IPV6 in Jamaica,» *IEEE*, 2018.

2

]

[Z. I. Gedeón, «ANALIZAR LA IMPORTANCIA DE INCORPORACIÓN DEL 8 COMPUTADOR COMO HERRAMIENTA,» *Laurus*, 2008.

3

]

[A. A. Sánchez, «El 89,9% de los hogares peruanos cuentan con al menos una 8 Tecnología de Información y Comunicación,» 28 Marzo 2016. [En línea]. Available: 4 [https://www.inei.gob.pe/prensa/noticias/el-899-de-los-hogares-peruanos-cuentan-](https://www.inei.gob.pe/prensa/noticias/el-899-de-los-hogares-peruanos-cuentan-con-al-menos-una-tecnologia-de-informacion-y-comunicacion-8975/)] con-al-menos-una-tecnologia-de-informacion-y-comunicacion-8975/.

[Mente Digital, «Influencia actual de las telecomunicaciones,» 08 Enero 2017. [En 8 línea]. Available: [https://www.amexempresas.com/libertadparatunegocio/influencia-](https://www.amexempresas.com/libertadparatunegocio/influencia-5-actual-las-telecomunicaciones/) 5 actual-las-telecomunicaciones/.

]

[M. Hilbert y P. López, «The World's Technological Capacity to Store, 8 Communicate, and Compute Information,» *Science*, 2011.

6

]

[Internet World Stats, «WORLD INTERNET USAGE AND POPULATION 8 STATISTICS,» 30 Junio 2018. [En línea]. Available:

7 <https://www.internetworldstats.com/stats.htm>.

]

[SpeedTest, «Speedtest Global Index,» Agosto 2018. [En línea]. Available:
8 <http://www.speedtest.net/global-index>.

8

]

[S. Aravind y G. Padmavathi, «Migration to Ipv6 From IPV4 by Dual Stack and
8 Tunneling Techniques,» *IEEE*, 2015.

9

]

[Y. Sookun y V. Basso, «Performance analysis of IPv4/IPv6 transition techniques,»
9 *IEE*, 2016.

0

]

[J. Vivas, C. Silva y J. L. Muñoz, «Implementation and Testing of IPv6 Transition
9 Mechanisms,» *IEEE*, 2017.

1

]

[M. Boucadair, M. Boucadair, M. Boucadair y M. Boucadair, «Migrating SIP-based
9 Conversational Services to IPv6: Complications and interworking with IPv4,» *IEEE*,
2 2007.

]

[M. H. Park, J. T. Kim y E. H. Paik, «Deployment Strategy and Performance
9 Evaluation of the IPv6 Home Network using the Home Server,» *IEEE*.

3

]