GUIA INFORMATIVA PARA LA IMPLEMENTACION DE SERVICIOS IPV4 A IPV6

YOHANA CATALINA RAMIREZ SARMIENTO
WILLIAMS YAHIR CAMACHO MENDEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE SISTEMAS
ESCUELA DE INGENIERÍA ELECTRICA, ELECTRONICA Y DE TELECOMUNICACIONES
ESPECIALIZACION TELECOMUNICACIONES
BUCARAMANGA
2013

GUIA INFORMATIVA PARA LA IMPLEMENTACION DE SERVICIOS IPV4 A IPV6

YOHANA CATALINA RAMIREZ SARMIENTO
WILLIAMS YAHIR CAMACHO MENDEZ

Trabajo de grado presentado como requisito para optar al título de Especialista en Telecomunicaciones

Director
FREDY BELTRÁN

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE SISTEMAS
ESCUELA DE INGENIERÍA ELECTRICA, ELECTRONICA Y DE TELECOMUNICACIONES
ESPECIALIZACION TELECOMUNICACIONES
BUCARAMANGA
2013

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

TITULO: **GUÌA INFORMATIVA PARA LA IMPLEMENTACIÒN DE SERVICIOS IPV4 A IPV6 ***

AUTORES: **YOHANA CATALINA RAMIREZ SARMIENTO ****
WILLIAMS YAHIR CAMACHO MENDEZ **

PALABRAS CLAVES: **Características, IPV4, IPV6, encabezado, direccionamiento, túneles, autoconfiguración, implementación.**

DESCRIPCIÒN:

El crecimiento exponencial de Internet ha pasado a formar parte de un medio de comunicación necesario y fundamental en las sociedades, debido a este gran aumento, las direcciones IPv4 se han agotamiento, esté factor ha impulsado la creación y adopción de diversas nuevas y mejoradas tecnología como lo es el Protocolo IPv6; el cual resuelve el problema de escasez de direcciones y proporcionan un numero prácticamente infinito de direcciones IP.

Actualmente en Colombia son pocas las empresas que se encuentran trabajando hoy en día sobre IPv6, algunas porque no han visto la necesidad de la migración de IPv4 a IPv6 y otras temen que los recursos informáticos de sus empresas no sean los suficientes para soportar el cambio.

En el capitulo cuatro de este documento se hace referencia al Modelo de Referencia TCP/IP, describiendo las capas de cada modelo, y realizando una comparación entre ambos modelos.

El capitulo cinco y seis, muestra los concepto del protocolo IPv4, sus características y aspectos básicos, igualmente se dan las generalidades respectivas a la función e importancia del protocolo de red IPV6, comparando los dos esquemas de direccionamiento y reflejando los múltiples servicios que abarca este nuevo protocolo.

El capitulo siete (7) no introduce en las definiciones, especificaciones y características del protocolo IPv6, describiendo completamente e introduciéndonos en el contexto del protocolo.

El ultimo capitulo del presente trabajo consiste en realizar una guía de los pasos a seguir para realizar una transición del protocolo IPv4 a IPv6 en una empresa, describiendo todos los aspectos a tener en cuenta en la planificación del proyecto al momento que las empresas requieran realizar la implementación del nuevo protocolo.

---

*Monografía

** Facultad de Sistemas, Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones. Director FREDY BELTRÁ

ABSTRACT

TITLE: **INFORMATION GUIDE FOR THE IMPLEMENTATION OF A SERVICE IPV4 IPV6 ***

AUTHORS: **YOHANA CATALINA RAMIREZ SARMIENTO ****
WILLIAMS YAHIR CAMACHO MENDEZ **

PALABRAS CLAVES: **Feature, IPV4, IPV6, header, addressing, tunnel, autoconfiguration, implementation.**

DESCRIPCIÒN:

The exponential growth of the Internet has become part of a means of necessary and critical communication companies, due to this large increase, the IPv4 address exhaustion have, be factor has driven the creation and adoption of various new and improved technology as what is the IPv6 protocol, which solves the problem of shortage of addresses and provide a virtually infinite number of IP addresses.

Currently in Colombia are few companies that are found working today on IPv6, some because they have not seen the need to of migration from IPv4 to IPv6 and other computing resources fear that their companies are not enough to support the change.

In chapter four of this document referring to Reference Model TCP / IP, describing the layers of each model, and making a comparison between the two models.

Chapter five and six, shows the concept of IPv4, features and protocol basics likewise the respective general to the role and importance of IPV6 network protocol are given, comparing the two addressing schemes and reflecting the many services covered by this new protocol.

The seven (7) does not introduce chapter in definitions, specifications and features of IPv6 protocol, fully describing and introducing in the context of the protocol..

The last chapter of this work is to make a guide to the steps to transition from IPv4 to IPv6 in an enterprise, describing all the aspects to consider in planning the project at the time that businesses require to perform implementation of the new protocol.

---

*Monograph
** Faculty of Systems Engineering School of Electrical, Electronic and Telecommunication.
Director FREDY BELT

INTRODUCCION

El actual crecimiento de la internet y el avance mundial en el uso de los dispositivos electrónicos móviles, de ahí surge la necesidad de mayor capacidad de direccionamiento IP, las direcciones IPv4 no fueron suficientes para cubrir las necesidades y perspectivas de crecimiento de los próximos años. Como consecuencia de esto se han desarrollado nuevas tecnologías y protocolos para solventar este problema. El Grupo Ingeniería de Internet (Internet Engineering Task Force o IETF, por sus siglas en inglés) elaboró una serie de especificaciones para definir un protocolo IP de siguiente generación (IP Next Generation, IPng) que actualmente se conoce como Protocolo de Internet versión 6.

El propósito de este documento es referenciar los conceptos relacionados con los dos protocolos, introduciéndonos en las generalidades y creando un marco de comparación, mostrando IPv6 como la herramienta de direccionamiento de nueva generación. Así mismo mostrar las consideraciones a tener en cuenta al comparar los esquemas de direccionamiento y establecer una guía básica para la implementación de este nuevo protocolo, de esta manera tener más claridad sobre los retos que nos propone realizar la transición de IPv4 a IPv6.

1. PLANTEAMIENTO DEL PROBLEMA

El siglo XXI, se caracteriza por el creciente acceso a la tecnología y por la globalización de la información y de la economía, el desarrollo tecnológico y el uso de Internet, proporcionan oportunidades y generan nuevos desafíos.

Las empresas están conectadas a través de grandes redes, las cuales mueven las diferentes estrategias de negocios, generando un desarrollo empresarial de grandes dimensiones. Estas redes están basadas en IPv4 (protocolo de internet versión 4) que posibilita 4.294.967.296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta y mucho menos a cada vehículo, teléfono, PDA, etc. En cambio IPv6 (Protocolo de internet versión 6) admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} o 340 sextillones de direcciones) cerca de $6{,}7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

He aquí la necesidad de empezar a dimensionar la transición, que debe existir en la tecnología, ya que IPv4 no puede soportar el crecimiento acelerado de las necesidades de conectividad, por lo tanto es necesario desarrollar una guía que ayude a hacer más ágil y fácil la migración de la misma.

Las empresas y los profesionales de tecnología que actualmente administran los diferentes centros de cómputo, están inseguros de realizar la migración, ya que no todas las empresas pueden permitirse cambiar su red o reprogramar sus aplicaciones para disponer de conectividad IPv6, a esto se añade la poca documentación e información de la nueva tecnología (IPv6), cuyos casos documentados de éxito de migración son escasos.

2. JUSTIFICACIÓN

Dado que IPv6 es un protocolo nuevo, que no es compatible con IPv4, y por ello IPv6 ha sido diseñado previendo un largo período de transición y co-existencia entre ambos. Es difícil definir durante cuánto tiempo ambos protocolos seguirán siendo utilizados en forma conjunta y en qué momento se dejara de utilizar IPv4, dado que depende de muchos factores, tanto técnicos como comerciales, podríamos decir que el mercado y la competencia marcarán la pauta.

La migración de una red IPv4 a IPv6 puede ser un proceso traumático para una organización, por tal motivo es necesario contar con alguna herramienta que permita darle un orden al proceso y que además permita identificar los puntos críticos del mismo. Normalmente los proveedores de servicio no realizan este acompañamiento, estos únicamente entregan los prefijos y se encargan de configurar sus enrutadores y es responsabilidad del cliente la configuración de su red interna.

En cualquier caso, se trata de una transición gradual y que ha de ser transparente para los usuarios, que poco a poco percibirán mejoras en aplicaciones existentes y otras nuevas, que no serían posibles con IPv4.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar una guía informativa que muestre en forma ordenada los pasos necesarios para realizar la migración de una red de datos operando en IPv4 a una red de datos que opere en doble Stack IPv4 e IPv6 y en cada uno de estos pasos indicar la compatibilidad o incompatibilidad de los principales productos comerciales o de dominio Público que se utilizan en los componentes de la red.

3.2 OBJETIVOS ESPECÍFICOS

1. Conocer cuáles son las características del nuevo protocolo IPv6, cuáles son los cambios en comparación con el anterior protocolo IPv4 y en base a esto, saber cuáles son los beneficios que trae IPv6.

2. Establecer los requisitos mínimos para que la operación de la organización funcione correctamente adoptando el nuevo protocolo. La nueva configuración debe ser capaz de comunicarse tanto con usuarios que siguen funcionando bajo IPv4 como con usuarios que ya hayan migrado a IPv6.

4. ARQUITECTURA O MODELO TCP/IP

El TCP/IP fue desarrollado y presentado en 1972 por el Departamento de Defensa de U.S., y fue aplicado en ARPANET (Advanced Research Projects Agency Network), que era la red de área extensa del Departamento de Defensa como medio de comunicación para los diferentes organismos de U.S. la transición hacia TCP/IP en ARPANET se concretó en 1983.

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de Transmisión / Protocolo Internet (TCP/IP). Se le conoce como familia de protocolos de Internet al conjunto de protocolos de red que son implementados por la pila de protocolos sobre los cuales se fundamenta Internet y que permiten la transmisión de datos entre las redes de computadores, desde cualquier parte del mundo a casi la velocidad de la luz

Los dos protocolos más importantes y que fueron los primeros en definirse y también los más utilizados, son **TCP** (Protocolo de Control de Transmisión o Transmission Control Protocol) e **IP** (Protocolo de Internet o Internet Protocol), de ahí que se denomine también como colección de protocolos estándar de la industria diseñada para intercomunicar grandes redes.

En conclusión se podría decir que TCP/IP es la plataforma que sostiene Internet y que permite la comunicación entre diferentes sistemas operativos en diferentes computadoras, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN). Así mismo la característica que hizo del modelo TCP/IP la arquitectura de red más popular en el mundo es la posibilidad que tienen las aplicaciones de correr sobre TCP/IP independientemente de las características físicas de la red.

El modelo TCP/IP consta de 5 niveles o capas, las cuales se pueden observar en la tabla 001, en la cual se reflejan las similitudes y diferencias con el modelo OSI

Tabla 1. Arquitectura o modelo TCP/IP

<table>
<tr><th rowspan="2">MODELO OSI</th><th colspan="4">TCP/IP</th></tr>
<tr><th colspan="3">Protocolos</th><th>Nivel</th></tr>
<tr><td>7 – Aplicación</td><td colspan="3" rowspan="3">FTP, HTTP, SSH, SSL, TELNET, SMTP, NFS, POP3, etc.</td><td rowspan="3">5 - Aplicación</td></tr>
<tr><td>6 – Presentación</td></tr>
<tr><td>5 – Sesión</td></tr>
<tr><td>4 – Transporte</td><td colspan="2">TCP</td><td>UDP</td><td>4 - Transporte</td></tr>
<tr><td>3 – Red</td><td>IP</td><td>ICMP</td><td>ARP, RARP</td><td>3 – Internet</td></tr>
<tr><td>2 – Enlace</td><td colspan="3">ETHERNET, CSMA, TOKEN-RING, ATM, etc.</td><td>2 – Acceso de la Red</td></tr>
<tr><td>1 – Física</td><td colspan="3">Cable coaxial, Cable de Fibra óptica, Cable de Par trenzado, Microondas, Radio, etc.</td><td>1 - Física</td></tr>
</table>

Normalmente, los tres niveles superiores del modelo OSI (Aplicación, Presentación y Sesión) son considerados simplemente como el nivel de aplicación en el conjunto TCP/IP. Como TCP/IP no tiene un nivel de sesión unificado para que los niveles superiores se sostengan, estas funciones son típicamente desempeñadas (o ignoradas) por las aplicaciones de usuario. La diferencia más notable entre los modelos de TCP/IP y OSI es el nivel de Aplicación, en TCP/IP se integran algunos niveles del modelo OSI en su nivel de Aplicación.

5. El PROTOCOLO IP

Más allá de los aspectos relacionados con el hardware de red de las maquinas como el acceso al adaptador de red y un mecanismo para la resolución de direcciones hardware el cual suministra acceso a nuestra red local, permitiendo la comunicación a nivel de trama con todas las máquinas de la misma. Sin embargo la necesidad de interconexión de distintas redes tanto locales como de área extensa o metropolitana; introduce el concepto del Protocolo IP (internet Protocol), el cual define un espacio de direcciones universales por encima de las direcciones hardware que cada red define, en otras palabras es un protocolo software que esta desligado de los detalles del hardware de red.

Una dirección IP es un identificador de cada host dentro de su red de datos, se caracteriza por ser exclusiva dentro de una misma área existente, las direcciones IP se caracterizan por conformarse en dos partes: una identifica la red y la otra identifica la maquina dentro de la red, se debe tener en cuenta que todas las maquinas que pertenecen a la misma red, requieren un mismo número de red el cual debe ser único en internet.

6. PROTOCOLO IPV4

IPV4 es la versión 4 del Protocolo de Internet (IP o Internet Protocol), es el protocolo de nivel de red usado en internet, que junto con otros protocolos auxiliares es responsable de transferir la información del usuario por la red, constituyendo la primera versión de IP que es implementada en forma extensiva.

IP es un protocolo ideado para interconexión de redes heterogéneas mediante routers. Se trata de un protocolo de conexión no fiable, que no garantiza la entrega segura de los paquetes. Además, los paquetes que se transmiten a la red, aunque pertenezcan a un mismo mensaje original, pueden seguir caminos diferentes, por lo que pueden llegar desordenados e incluso duplicados. Deberá ser la capa de transporte, o incluso la propia aplicación, la que, en su caso, detecte y resuelva todas estas situaciones de error.

En una red, cada host tiene asignada una dirección IP única que se utiliza para establecer comunicación con otros hosts en dicha red, las direcciones se expresan en formato decimal separado por puntos (25.120.240.100). Cada parte de una dirección se constituye de 4 números de 8 bits cada un octetos en binario, equivalentes a decimales desde 0 a 255, como consecuencia, habrá un máximo de 232 = 4.294.967.296 direcciones únicas disponibles para uso en el caso de las direcciones IPv4. Por tanto, una dirección IP es un número que identifica de manera lógica una interfaz de red. Sin embargo, un gran número de direcciones se reservan para uso local y, por ello, no están disponibles para Internet.

6.1 CLASES DE DIRECCIONES IP

Este esquema de direcciones tiene como características fundamentales: se divide en dos (2) partes, una que corresponde a la dirección de la red o subred a la que

pertenece le host y otra a la dirección del propio host; se crearon cinco (5) clase de direcciones A, B, C, D y E, en donde solo se pueden usar las tres (3) primeras clases. Adicionalmente cada dirección IP debe estar acompañada por una dirección IP especial conocida como máscara de subred, la cual indica los bits de la dirección IP que identifican la red y los que identifican host.

Una red de clase A se reserva, generalmente para los Gobiernos, aunque también llegó a hacerse para empresas transnacionales. Las direcciones de clase B se otorgan a medianas empresas. Los usuarios “normales” usarán direcciones de clase C, las direcciones de clase D se usan para multidifusión (multicast) y las direcciones clase E, Se reservan únicamente para investigación. Los números de direcciones de red los administra la ICANN (Corporación de Internet para la Asignación de Nombres y Números) a fin de evitar conflictos.

Tabla 2. Clases de direcciones IP

CLASE	FORMATO				RANGO
A	RED	HOST	HOST	HOST	0.0.0.0 a 127.255.255.255
B	RED	RED	HOST	HOST	128.0.0.0 a 191.255.255.255
C	RED	RED	RED	HOST	192.0.0.0 a 233.255.255.255
D	ID GRUPO MULTICAST				224.0.0.0 a 239.255.255.255
E	EXPERIMENTAL				240.0.0.0 a 247.255.255.255

Además de las clases de direcciones, también se encuentran la división que se hacen entre IP Publicas e IP privadas, las primeras visibles a internet accesibles desde cualquier otro host conectado y las otras usadas para organizaciones privadas, son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por enrutadores, sin embargo desde internet no se puede acceder directamente a computadoras con direcciones IP privadas.

6.2 CARACTERÍSTICAS DE IPV4

IP o protocolo de Internet es un protocolo no orientado a conexión, poco confiable que su principal función es el direccionamiento y crear paquetes que puedan ser encaminados entre estaciones. No orientado a conexión significa que la conexión no es establecida antes de comenzar a transmitir datos. Poco confiable se refiere a que la entrega de los paquetes no es garantizada, estos trabajos son responsabilidad de las capas superiores y por ello IP no lo ejecuta.

6.2.1 Dirección de 32 bits. Son 4.294.967.296 direcciones disponibles. Dentro de este gran número de direcciones, hay un gran espacio reservado para usos locales y existe una asignación por clases. La dirección se compone de 4 octetos de números del 0 al 255 separados por puntos, por ejemplo 66.230.200.255.

6.2.2 Direccionamiento y enrutamiento. El protocolo IP es un protocolo enrutado el cual ofrece direccionamiento, fragmentación y reensamblaje de datagramas y entrega de datagramas a través de la interred. Una dirección IP en versión 4 está compuesto por 4 campos de 8 bits y cada campo es separado por un punto “.”. El direccionamiento IP o direccionamiento de capa de internet es necesario para poder identificar a una interfaz de un dispositivo con una única dirección como miembro de una red en específico, pues la identificación de un nodo en una interred requiere el uso de la red a la que pertenece y la identificación del nodo en dicha red.

7. PROTOCOLO DE INTERNET VERSION 6 (IPv6)

La versión 6 del protocolo para internet se denominó (IPV6) fue adoptado a finales del año 1994 para la Internet Engineering Task Force (IEFT), luego de realizar las pruebas iniciales de la versión 5 las cuales no pasaron la fase experimental, este nuevo protocolo de internet también llamado IP Next Generation o (IPng).

Las modificaciones que se introducen en este nueva versión han sido diseñadas para dar solución a todos los problemas estructurales que surgieron para la versión 4, así mismo para soportar nuevas redes de comunicación de alto rendimiento, igualmente es de destacar que a nivel mundial con el paulatino crecimiento de aplicaciones, unido a las nuevas generaciones en telefonía móvil que funcionaran sobre IP, se hace necesario direcciones IP publicas globales y válidas para conexiones extremo a extremo “enrutables”, las suma de todos estos conceptos hacen que la transición del IPv4 a IPv6 sea impostergable.

7.1 CARACTERÍSTICAS PRINCIPALES DE IPV6 CON RESPECTO A IPV4

A continuación se muestran las características en las cuales ha evolucionado el protocolo de internet en su nueva versión 6 en respuesta a las falencias evidenciadas por IPv4.

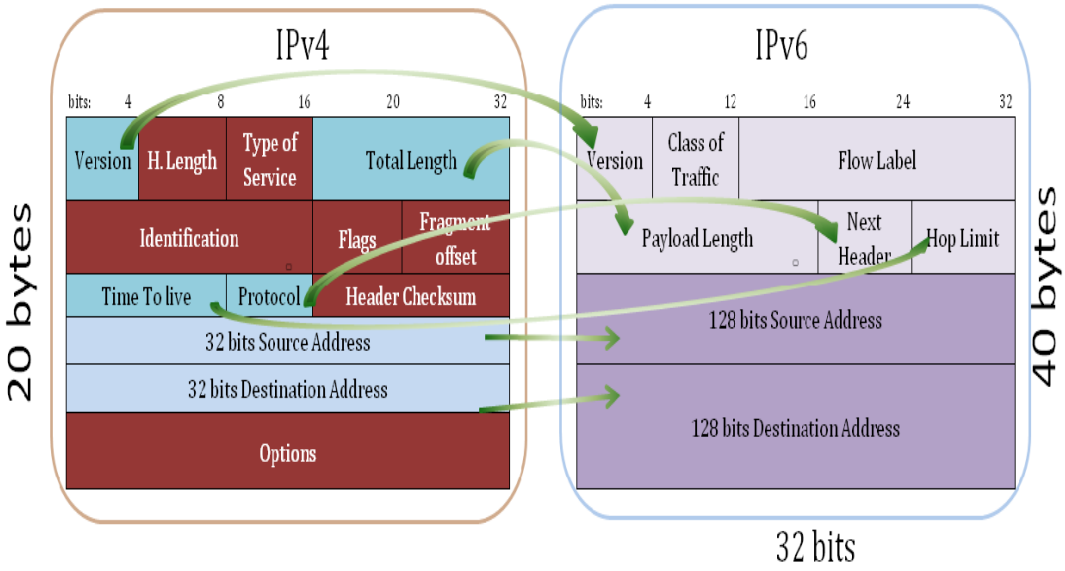
7.2 ESPACIO DE DIRECCIONES

Las representación de las direcciones cambian enormemente y pasan de estar representadas por direcciones de 32 bits lo que significa 2^{32} = 4.294.9679296 direcciones posibles, a 128 bits, esta es considerada un de las principales características de IPv6 aportado un espacio de 2^{128} direcciones equivalentes a 3.40×10^{38} esto es 340 sextillones de direcciones, esto ha sido diseñado para

establecer varios niveles de subredes y asignaciones de redes de la red troncal de Internet. Por lo tanto las técnicas de conservación de direcciones, como las distribuciones de NAT para IPv4 ya no son necesarias.

7.3 FORMATO DE CABECERA

Figura 1. Formato de cabecera



Se realizan algunas modificaciones en el formato de la cabecera de IPv4 reflejando algunos principios operacionales nuevos que se introducen en IPv6, la cabecera del datagrama IP ha pasado de tener 12 campos en IPv4 a tener solo 8 en IPv6, en conclusión posee menor cantidad de campos, sus estructura y contenidos han sido mejorados; optimizando los recursos que utiliza, pues se han eliminado algunos campos repetitivos que ya se representaban anticuados, incrementando algunas características para hacer frente a las nuevas necesidades de las redes actuales, como comunicación en tiempo real y seguridad.

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o longitud sin embargo, para simplificar la vida de los enrutadores, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos como se muestra en la figura 001

El campo Versión: es de 4 bits de largo e identifica la versión del protocolo, se puede observar que este es el único campo con una función y posición que es consistente entre IPv4 e IPv6. Este campo al comienzo del paquete permite una rápida identificación de la versión del IP y el paso de ese paquete al protocolo de proceso apropiado bien sea IPv4 o IPv6; durante el periodo de transición entre las versiones, los routers deberán fijarse en este campo para saber qué tipo de datagrama están enrutando.

7.3.1 El campo Traffic Class. Es de 8 bits de largo y su intención para los nodos de origen y/o nodos de reenvío es identificar y distinguir entre diferentes clases o prioridades de paquetes IPv6. Este campo reemplaza las funciones que fueron suministradas por el campo Type of Service de IPv4, permitiendo la diferenciación entre categorías del servicio de transferencia de paquetes. Esta función es comúnmente referida como “Servicio de Diferenciación”.

Traffic Class se utiliza para distinguir las fuentes que deben beneficiarse del control de flujo de otras. Se asignan prioridades de 0 a 7 a fuentes que pueden disminuir su velocidad en caso de congestión; se asignan valores de 8 a 15 al tráfico en el tiempo real (datos de audio y video incluidos) en donde la velocidad es constante. Esta distinción en los flujos permite que los routers reaccionen mejor en caso de congestión. En cada grupo de prioridad, el nivel de prioridad más bajo se relaciona con los datagramas de menor importancia.

7.3.2 El campo Flow Label. Es de 20 bits de longitud, y puede ser usado por un host para solicitar manejo especial para ciertos paquetes, como aquellos con una calidad de servicio de no default o de tiempo real.

Un flujo es una secuencia de paquetes enviados a un destino unicast o multicast que necesita manejo especial por los routers IPv6 que intervienen; todos los paquetes pertenecientes a un mismo flujo debe ser enviado con la misma dirección fuente, dirección destino y etiqueta de flujo. Un ejemplo de un flujo sería paquetes que soportan un servicio en tiempo real, como audio o vídeo. Flow Label es usado por esa fuente para etiquetar esos paquetes que requieren manejo especial por el nodo IPv6, si un host o router no soporta funciones de Flow Label, el campo es fijado a cero en el origen e ignorado en la recepción.

Múltiples flujos de datos pueden existir entre una fuente y un destino, así como tráfico de datos que no es asociado con un flujo particular. Un flujo único es identificado por la combinación de una dirección fuente y una etiqueta de flujo que no sea cero. La etiqueta de flujo es un número seudo-aleatorio elegido del rango de 1 a FFFFFH (donde H denota notación hexadecimal). Esa etiqueta es usada como una clave hash por router para buscar el estado asociado con ese flujo.

7.3.3 El campo Payload Length. Es un entero no asignado de 16 bits, indica el tamaño o la longitud de la carga útil del paquete, las cabeceras adicionales son consideradas parte de la carga para este cálculo, junto con cualquier protocolo de capa más alta, como TCP, FTP, etc.

El campo Payload Length es similar al campo Total Length de IPv4, excepto que las 2 medidas operan en diferentes campos. Payload Length (IPv6) mide los datos, después del encabezado, mientras Total Length (IPv4) mide los datos y el encabezado.

7.3.4 El campo Next Header. Tiene 8 bits de longitud e identifica el encabezado inmediatamente siguiente del encabezado de IPv6, puede ser un protocolo de una capa superior o una extensión. Este campo usa los mismos valores que el campo Protocol de IPv4. Las sucesivas cabeceras no son examinadas en cada nodo de la ruta, sino solo en el nodo o nodos destinos finales. Hay una excepción a esta regla y se presenta cuando el valor de este campo es 0, lo que indica opción de examinado y proceso salto a salto.

7.3.5 El campo Hop Limit. Tiene 8 bits de longitud, y va decreciendo en 1 por cada nodo que reenvía el paquete. Cuando Hop Limit se iguala a cero, el paquete es descartado y un mensaje de error es retornado. Este campo es similar al campo Time-to-Live (TTL) encontrado en IPv4, con una excepción clave. El campo Hop Limit (IPv6) mide el máximo de saltos (hops) que pueden ocurrir mientras el paquete es enviado por varios nodos. El campo TTL (IPv4) puede ser medido en saltos o segundos, algo importante es que con Hop Limit usada en IPv6, la base del tiempo no está disponible más.

Los siguientes campos son Source Address y Destination Address. Después de diferentes debates, se acordó que lo mejor era que las direcciones tuvieran una longitud fija equivalente a 16 bytes. Los primeros bits de la dirección el prefijo definen el tipo de dirección. Las direcciones que comienzan con 8 ceros se reservan, en particular para las direcciones IPv4. Se admiten dos variantes, que se distinguen según los 16 bits siguientes (o sea 16 bits a 0 ó 1).

La ventaja principal de este incremento en el espacio de direcciones se refleja, sobre todo, en que se elimina la limitación actual de disponibilidad de direcciones IP y los métodos artificiales para evitar dicha limitación como, por ejemplo, NAT (Network address translation). La principal desventaja de este aumento del número de direcciones es la sobrecarga en el ancho de banda utilizado debido al

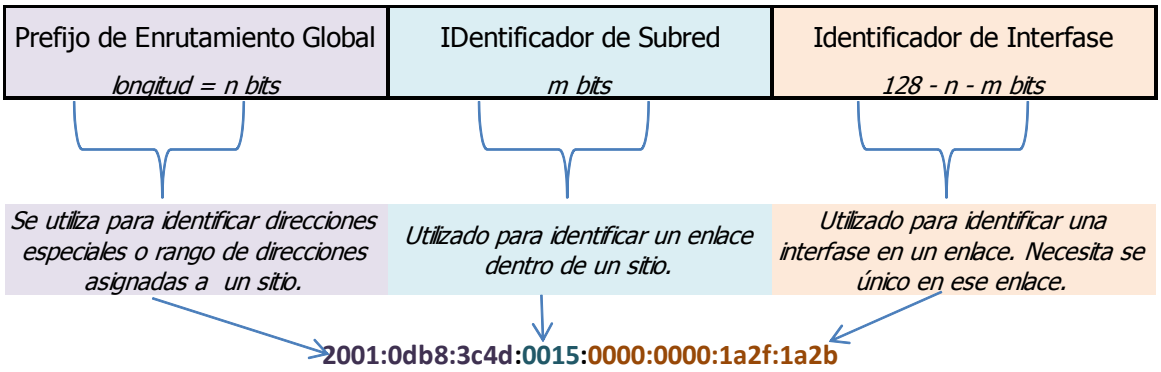
incremento del tamaño de la cabecera de los paquetes. Esta sobrecarga se puede aliviar utilizando la opción de compresión de las cabeceras de los mensajes.

7.4 DIRECCIONAMIENTO IPV6

Las Dirección IPv6 son asignadas a interfaces, no a nodos, por lo que cada interface de un nodo necesita al menos una dirección unicast. A una sola interfase se le pueden asignar múltiples direcciones IPv6 de cualquier tipo (unicast, anycast, multicast). Por lo cual un nodo puede ser identificado por la dirección de cualquiera de sus interfases.

Una dirección típica de IPv6 consiste en tres partes como se muestra en la figura 002.

Figura 2. Direccionamiento IPv6



Los primeros tres campos a la izquierda (48 bits) contienen el prefijo de sitio, este describe la topología publica que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el ID de subred de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la topología privada, denominada también topología del sitio, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el ID de interfaz, también denominado token. El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Examine de nuevo la dirección de la Figura 002:

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

En este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, 2001:0db8:3c4d, contienen el prefijo de sitio y representan la topología pública. Los siguientes 16 bits, 0015, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, 0000:0000:1a2f:1a2b, contienen el ID de interfaz.

7.5 REPRESENTACIÒN DE DIRECCIÒN IPV6

Las direcciones IPv6 se referencian por 8 campos de 16 bits cada uno, separados por dos puntos ":", y cada 4 números hexadecimales son usados para representar cada sección de 16 bits, como por ejemplo.

2001:0db8:85a3:0000:0000:8a2e:0370:7334.

La notación IPv6 se puede simplificar con las siguientes reglas que afectan a los ceros:

- **Ceros Iniciales:** los ceros iniciales de cada grupo pueden omitirse, de ese modo las direcciones IPv6 se escriben (2001:db8:85a3:0:0:8a2e:370:7334). Cada grupo debe contener al menos un digito hexadecimal.

- **Grupos de Ceros:** Si aparecen largas cadenas de ceros en una dirección, se sustituyen en (::) lo cual puede ser usado para indicar múltiples grupos de 16 bits de ceros, que luego simplifican la dirección a (2001:db8:85a3::8a2e:370:7334). El uso de "::" es restringido al aparecer solo una vez en una dirección, aunque puede ser usado para comprimir o los ceros del principio o los subsiguientes en una dirección.

7.6 DIRECCIÒN IPV6 COMPATIBLE CON IPV4

Es utilizada para establecer un túnel automático que lleva paquetes IPv6 sobre redes IPv4. Esta dirección está vinculada con un mecanismo de transición del protocolo IPv6.

7.7 DIRECCIONES IPV4-MAPEADA

Se utiliza sólo en el ámbito local de nodos que tienen las direcciones IPv4 e IPv6. Los nodos usan direcciones IPv6 mapeadas a IPv4 de forma interna solamente. Estas direcciones no son conocidas afuera del nodo y no llegan al cable de comunicación como direcciones IPv6. Se ha introducido una notación especial para expresar direcciones IPv6 que sean IPv4-mapeada, representando los últimos 32 bits de la dirección IPv6 en el formato decimal con puntos usado en IPv4, por ejemplo; (::ffff:c000:280 se puede representar como ::ffff:192.0.2.128).

Como se menciona cada campo es expresada en notación hexadecimal; esto implica mayor necesidad e importancia del servicio DNS, debido a la dificultad que implica memorizar una dirección del tamaño de las direcciones IPv6.

7.8 REPRESENTACIÓN DE LOS PREFIJOS DE LAS DIRECCIONES IPV6

El prefijo es la parte de la dirección que indica los bits que tienen valores fijos o reflejan el identificador de subred. Los prefijos de las rutas e identificadores de subred IPv6 se expresan de la misma forma que la notación CIDR (Enrutamiento de interdominios sin clases) de IPv4, se representa como:

= IPv6-address/prefix-length

7.8.1 IPv6 address. Es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.

7.8.2 Prefix-Length. Es un valor decimal especificando cuántos de los bits, colocados más a la izquierda, de la dirección comprenden el prefijo, representando el prefijo de la dirección.

Como se mencionó el tamaño del prefijo se expresa en notación CIDR (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo en bits.

El prefijo de sitio de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48 se ubica en los 48 bits que hay más a la izquierda, 2001:db8:3c4d. Se utiliza la representación con ceros comprimidos, para representar este prefijo 2001:db8:3c4d::/48.

También se puede especificar un prefijo de subred, que define la topología interna de la red respecto a un enrutador. La dirección IPv6 de ejemplo tiene el siguiente prefijo de subred: 2001:db8:3c4d:15::/64. El prefijo de subred siempre contiene 64 bits. Estos bits incluyen 48 del prefijo de sitio, además de 16 bits para el ID de subred.

Las implementaciones de IPv4 suelen usar una representación decimal con punto del prefijo de red, que se conoce con el nombre de máscara de subred. En IPv6 no se usan máscaras de subred. En IPv6 sólo se admite la notación con longitud del prefijo.

7.9 DIRECCIONAMIENTO JERÀRQUICO E INFRAESTRUCTURA DE ENRUTAMIENTO EFICIENTES EN IPV6.

Con IPv4 se desplegaron complejas técnicas de classless interdomain Routing (CIDR) para utilizar de mejor manera el pequeño espacio de direcciones; el esfuerzo requerido para reasignar la numeración de una red existente con prefijos de rutas distintos es muy grande. La nueva versión se diseña para crear una infraestructura de enrutamiento jerárquica eficiente, que se basa en la ocurrencia común de múltiples niveles de proveedores de servicios de internet, lo que significa mejor agregación de rutas y reducción en el tamaño de la tabla de enrutamiento de los routers de red troncal. Sin embargo hubiera sido muy fácil solamente aumentarle bits a las direcciones de la versión 4 para tener más direcciones, pero al tener mayor número de direccione el problema radicaría en el enrutamiento a través de Internet, para este caso IPv6 se definieron tres tipos de direcciones.

7.9.1 UNICAST – "Unidistribución". Identificador para una Única Interfaz; Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada con dicha dirección; es el equivalente a las direcciones IPv4 actuales. En IPv6, las direcciones unicast pueden pertenecer a uno de los tres contextos existentes:

- **Local al enlace ("link-local")**. Son aquellas que permiten la comunicación entre los distintos nodos conectados a un mismo enlace capa 2 del modelo

ISO/OSI. Estas direcciones no pueden ser enrutadas y sólo son válidas al interior del enlace. Cada vez que un nodo IPv6 se conecta a una red, adquiere automáticamente una dirección local al enlace, sin ser necesaria la intervención del usuario o de otros dispositivos. Así mismo permiten proveer de forma rápida y simple conectividad entre los nodos conectados a un mismo enlace. Su principal ventaja es que no dependen de los prefijos IPv6 anunciados en una red, por lo que permiten identificar directamente a los nodos y "routers" presentes en un enlace.

- **Local único ("unique-local")**. Son direcciones que permiten la comunicación de nodos al interior de un sitio. Se entiende por sitio a toda red organizacional, de prefijo /48, compuesta por 1 o más subredes. Son el equivalente a las direcciones privadas en IPv4, cumpliendo la misma función: proveer conectividad entre los nodos de un sitio o "intranet". Al igual que las direcciones locales al enlace, no pueden ser enrutadas hacia Internet.

- **Global.** Son usadas para comunicar 2 nodos a través de Internet. Son el equivalente a las direcciones públicas en IPv4. Son el único tipo de direcciones que pueden ser enrutadas a través de Internet. El espacio reservado actualmente para este tipo de direcciones es de 2001: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001::/3). Todas las subredes en el espacio de direccionamiento unicast global tienen un prefijo de red fijo e igual a /645. Esto implica que los primeros 64 [bit] (los primeros 4 campos en formato hexadecimal) corresponden al identificador de red, y los siguientes corresponden a la identificación de la interfaz de un determinado nodo.

El prefijo de enrutamiento global es aquel que identifica a un sitio conectado a Internet. Dicho prefijo sigue una estructura jerárquica, con el fin de reducir el tamaño de la tabla de enrutamiento global en Internet.

7.9.2 Anycast – "Monodistribución". Identificador para múltiples interfaces pertenecientes a diferentes nodos, un paquete enviado a una dirección anycast es entregado en una de las interfaces identificadas con dicha dirección, de acuerdo a la distancia establecida por el protocolo de encaminado. La cual permite crear un ámbito de redundancia de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada, si la primera cae.

7.9.3 Multicast – "Multidistribucion". Opera de la misma forma que ne IPv4, es un identificador para un conjunto de interfaces pertenecientes a diferentes nodos; un paquete enviado a una dirección multicast es entregado a todos las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast). La arquitectura de direcciones es más simple y fija, lo cual permite una fácil planificación y con ello se reduce el costo de manejo de las redes; e IPv6 las máscaras de subred son fijas y proveen una virtual cantidad ilimitada de nodos en un enlace.

El uso de "anycast" permite entre otras cosas implementar balanceo de carga y tolerancia a fallas. Por lo general, su uso se suele restringir al contexto de un sitio o red local. Las direcciones "anycast", al igual que las "multicast" solo son válidas como direcciones de destino en los paquetes IPv6.

7.10 ASIGNACIÓN DE DIRECCIONES IPV6

El delegado para la asignación del direccionamiento IPv6 en la Internet Assigned Numbers Authority (IANA). Su función principal es la asignación de grandes bloques de direcciones a los Registros Regionales de Internet (RIRs por sus siglas en inglés), que tienen la tarea de asignar trozos menores a Proveedores de Internet u otros registros locales.

Actualmente, sólo la octava parte del espacio total de direcciones están disponibles para su uso en Internet. La mayor parte de las direcciones IPv6 están reservadas para uso futuro. Para conseguir agregación de rutas, reduciendo así el tamaño de las tablas de rutas de Internet, el rango 2000::/3 se asigna a los RIRs en grandes bloques desde /23 hasta /12.14

Los RIRs asignan rangos menores a ISPs (Proveedor de Servicios de Internet), que luego distribuyen en bloques de /48 a sus clientes. Las direcciones IPv6 se asignan a las organizaciones en bloques mucho mayores a las asignaciones IPv4; la asignación recomendada es un rango /48, que es 248 ó 2.8×1014 veces mayor que el direccionamiento IPv4 completo. A pesar de ello, el conjunto total es suficiente para el futuro previsible, pues hay 2128 ó sobre 3.4×1038 direcciones IPv6.

Cada RIR puede dividir cada uno de sus bloques /23 en 512 bloques /32, normalmente uno para cada ISP. Un ISP puede dividir cada uno de sus rangos /32en 65.536 bloques /48, normalmente uno para cada cliente. Los clientes pueden crear 65.536 redes /64 con su asignación /48, teniendo cada red un número de direcciones que es el cuadrado de todo el espacio de direcciones IPv4, que sólo tenía 232 ó 4.3×109 direcciones.

Tal y como se ha diseñado, sólo una pequeña fracción del espacio de direcciones se utilizarán realmente. El amplio espacio de direcciones asegura que prácticamente siempre habrá disponibilidad, lo que convertirá a la traducción de direcciones (NAT) en innecesaria desde un punto de vista de direccionamiento. NAT se utiliza actualmente sobre todo para aliviar el agotamiento de las direcciones IPv4, pero también tiene aspecto económico ya que el alquiler de direcciones IP tiene un coste. Desde un punto de vista de la seguridad evita exponer información de estructura y gestión interna de red hacia internet.

7.11 CRITERIOS PARA ASIGNAR DIRECCIONES IPV6

Una vez obtenido un prefijo de red por un RIR se debe trazar un plan de direccionamiento para dotar de dirección nuestras máquinas/redes. Dicha asignación es para las diferentes redes y subredes existentes.

Para ello se pueden considerar los siguientes criterios:

– Todas las redes internas que vayan a desplegar IPv6 tendrán un prefijo /64. Necesario para la construcción automática de direcciones IPv6 de tipo Unicast y/o Anycast

– Los usuarios finales, clientes residenciales (acceso xDSL, FTTx, etc.), como corporativos (empresas, ISPs, Universidad, etc.) podrán recibir prefijos de longitud /48, dejando 16 bits del bloque de red para crear subredes.

La siguiente tabla muestra los prefijos IPv6 comunes y el número de subredes IPv6 y direcciones IPv6 que admiten.

Tabla 3. Criterios para asignar direcciones IPV6

Prefijo	Numero de Subredes
/64	1 subred IPv6 con hasta 18.446.744.073.709.551.616 direcciones IPv6 host
/56	Subredes 256 /64
/48	Subredes 65.536 /64

En IPv6, la notación diagonal se utiliza para representar el prefijo identificador de red para una red IPv6. El prefijo se representa con una barra diagonal (/), seguida por el tamaño del prefijo que es un número decimal entre el 1 y el 128. La notación CIDR funciona exactamente del mismo modo que con IPv4, lo que significa que si posee un /48, entonces los primeros 48 bits de la dirección son el prefijo. Un sitio

de red al que se le asigna un prefijo /48 puede usar prefijos en el rango de /49 a /64 para definir subredes válidas.

7.12 SUBREDES EN IPV6

Los proveedores e ISP que se encuentran en el proceso de implantación de la nueva versión del protocolo IP, sigue las instrucciones del RIPs respecto a cómo repartir el enorme espacio de direccionamiento IP versión 6 entre sus clientes. Existe una diferencia muy grande entre las recomendaciones para la asignación de las direcciones IP versión 4, que busca ante todo la economía de direcciones, pues como es sabido falta muy poco tiempo para que se agoten, y las de la versión 6 que busca la flexibilidad.

Sin embargo, con IPv6 el cliente recibiría una subclase como la siguiente: 2001:0ba0:1c01::/48; dicho cliente puede a su vez crear en sus instalaciones 65.535 subredes diferentes, que son las combinaciones creadas variando w,x,y,z en el grupo: 2001:0ba0:01b0:wxyz::/64, cada una de esas 65.535 subredes que nuestro cliente puede crear, puede a su vez tener más de 18 trillones de direcciones IP diferentes, que pueden ser de asignación automática (plug and play) o manual por el cliente.

7.13 CREAR SUBREDES CON IPV6

1. Se define un ámbito de direcciones IPv6. IPv6 es una dirección de 128 bits con los primeros 48 bits de Internet dedicados a la ruta, los siguientes 16 bits dedicados a las subredes y los últimos 64 bits dedicados a los huéspedes. Un ejemplo de una dirección IPv6 es 10:0:0:0:0:0:24:4b0 con una máscara de subred de FFFF: FFFF: FFFF: FFFF: 0:0:0:0. Esto también se puede representar como 10 :: 24:4b0/16.

2. Implementa la dirección IPv6 y la máscara de subred. Los 16 bits en el cuarto octeto se dedican a la división en subredes, dando subredes 65.535 con más de 18 trillones de huéspedes por subred. Sólo el cuarto octeto de la máscara de subred debe ser manipulado por el gran número de subredes y huéspedes puestos a disposición por una dirección IPv6.
3. Cambia los bits en el cuarto octeto para configurar una subred. Usar la máscara de subred FFFF: FFFF: FFFF: FFFF: 0:0:0:0, una dirección IPv6 tal como 10 :: 1:0:0:24:4 B0 está en una subred diferente a la 10 :: 02:00: 0:24:4 B0. El número de bits para el direccionamiento del nodo dentro de un prefijo de sitio (48 bits) en IPv6 resulta ser tan grande que no es necesario hacer un plan de direccionamiento para un sitio utilizando diferentes valores de máscara de red; de ahí que el cálculo de máscara de red para cada subred y el uso de VLSM no son requeridos.

7.14 AUTOCONFIGURACIÓN EN IPV6

Además de la configuración manual en IPv4, si se desea que los hosts se autoconfiguren, hay que utilizar el protocolo DHCP (Dynamic Host Configuration Protocol) perteneciente a la capa de aplicación. Mediante este protocolo, los hosts le preguntan a los routers de la red que estén escuchando peticiones DHCP qué IP pueden asignarse y qué opciones de configuración deben utilizar.

En la versión 6, la autoconfiguración se conceptualiza como el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces, este mecanismo permite afirmar que IPv6 es “Plug & Play”. Este proceso crea una dirección de enlace local, verificando la no duplicidad en dicho enlace y determinando la información que ha de ser autoconfigurada.

En IPv6, esta característica está incluida en la propia capa de red autoconfiguración "stateless") y no se necesita de software adicional para

proporcionarla, aunque también se puede utilizar DHCPv6, el equivalente a DHCP pero para IPv6, si se quiere mantener el anterior modelo de autoconfiguración (autoconfiguración "stateful"). Ambos tipos de autoconfiguración pueden convivir perfectamente en la misma red. Es frecuente usar la autoconfiguración "stateless o sin estado" para conseguir una IPv6 y después usar la autoconfiguración "stateful o con estado" para conseguir otros parámetros de configuración, como por ejemplo, los servidores DNS disponibles en esa red.

El hecho de que el mecanismo de autoconfiguración esté incluido en el propio protocolo IPv6 facilita mucho la adopción de esta tecnología por parte de dispositivos que no sean ordenadores personales o servidores, como pueden ser teléfonos móviles, electrodomésticos, consolas de videojuegos, etc. Esta característica les permite autoconfigurarse en cuanto estén en una red, ya sea cableada o inalámbrica, sin necesidad de ninguna manipulación por parte de los usuarios. En el caso de los routers, no se pueden utilizar estos mecanismos de autoconfiguración, ya que los se deben configurar manualmente y de forma estática, para que puedan servir de referencia a los demás hosts de la red a la hora de autoconfigurarse.

7.14.1 Configuración Stateful (Con estado o Configuración Predeterminada). Es la asignación de la dirección y sus parámetros correspondientes, siempre y cuando sean configurados con antelación, por medio de un servicio de asignación dinámico, mejor conocido como DHCPv6. Este tipo de autoconfiguración está diseñada específicamente para el uso de host o estaciones, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente. Además, los routers también tienen que aprobar el algoritmo de detección de direcciones duplicadas.

7.14.2 Configuracion Stateless (Sin Estado). En esta configuración, el host utiliza el prefijo (la dirección de red y la máscara de subred), el cual es “publicado” por los dispositivos de red o routers, como parte de la creación de la dirección. Posteriormente los clientes pueden utilizar su dirección física (MAC address) para completar la identificación del dispositivo y así asignar la dirección IPv6.

En este mecanismo no importa la dirección exacta que se asigna a un host, sino tan solo para determinar que es única y correctamente enrutable. Aun cuando el cliente puede generar automáticamente la dirección, no tiene conocimiento de ningún otro parámetro que pueda necesitar. Los dispositivos de red pueden ser configurados para “indicarle” al cliente donde y como puede obtener dichos valores.

7.15 DESCRIPCIÓN GENERAL DEL PROTOCOLO ND DE IPV6

En IPv6, el Protocolo de Resolución de Direcciones (ARP) en IPv4, es reemplazado por el protocolo de descubrimiento de nodos vecinos o ND (Neighbor Discovery), este protocolo es el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros en su mismo enlace, determinando sus direcciones en la capa de enlace, localizando los routers y manteniendo la información de conectividad acerca de las rutas a los vecinos activos. Así mismo el protocolo ND es empleado para mantener limpios los caches donde se almacena la información referente al contexto de la red a la que está conectada un servidor o un router, y para detectar cualquier cambio en la misma. Si un router o una ruta falla, el servidor buscará alternativas funcionales.

El protocolo ND controla principalmente las siguientes actividades del vínculo local de IPv6:

- **Descubrimiento de enrutadores**: ayuda a los hosts a detectar enrutadores en el vínculo local.
- **Configuración automática de direcciones**: permite que un nodo configure de manera automática direcciones IPv6 para sus interfaces.
- **Descubrimiento de prefijos**: posibilita que los nodos detecten los prefijos de subred conocidos que se han asignado a un vínculo. Los nodos utilizan prefijos para distinguir los destinos que se encuentran en el vínculo local de los asequibles únicamente a través de un enrutador.
- **Resolución de direcciones**: permite que los nodos puedan determinar la dirección local de vínculo de un vecino solamente a partir de la dirección IP de los destinos.
- **Determinación de salto siguiente**: utiliza un algoritmo para establecer la dirección IP de un salto de destinatario de paquetes que está más allá del vínculo local. El salto siguiente puede ser un enrutador o el nodo de destino.
- **Detección de inasequibilidad de vecinos**: ayuda a los nodos a establecer si un nodo ya no es asequible. La resolución de direcciones puede repetirse tanto en enrutadores como hosts.
- **Detección de direcciones duplicadas**: permite que un nodo pueda determinar si está en uso o no una dirección que el nodo tenga la intención de utilizar.
- **Redirección**: un enrutador indica a un host el mejor nodo de primer salto que se puede usar para acceder a un determinado destino.

Igualmente éste protocolo, ND emplea cinco (5) mensajes ICMPv6 para algunos de sus servicios:

- Solicitud de router
- Anunciación de router
- Solicitud de vecino
- Anunciación de vecino
- Redirección.

En conclusión el Protocolo de descubrimiento de vecinos IPv6 corresponde a una combinación de los protocolos IPv4 como: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Router Discovery (RDISC), e ICMP Redirect. Los enrutadores de IPv6 utilizan el protocolo ND para anunciar el prefijo de sitio de IPv6. Los hosts de IPv6 utilizan el descubrimiento de vecinos con varias finalidades, entre las cuales está solicitar el prefijo de un enrutador de IPv6.

7.16 COMPATIBILIDAD DE APLICACIONES CON DIRECCIONES IPV6

Muchos de los principales servicios de red reconocen y admiten direcciones IPv6; por ejemplo:

- Servicios de nombres como DNS, LDAP y NIS.
- Aplicaciones de autenticación y protección de la privacidad, por ejemplo IP Security Architecture (IPsec) e Internet Key Exchange (IKE).
- Servicios diferenciados, como los que proporciona IP Quality of Service (IPQoS).
- Detección de fallos y funcionamiento a prueba de fallos, como se proporciona mediante IP multirruta de redes (IPMP).

7.17 OTROS RECURSOS DE IPV6

Además de esta parte, hay información adicional sobre IPv6 en las fuentes que se citan en las secciones siguientes.

Hay disponibles numerosas RFC referidas a IPv6. En la tabla siguiente aparecen los principales artículos y sus ubicaciones web de Internet Engineering Task Force (IETF) a partir de su escritura.

Tabla 4. Otros recursos de IPV6

RFC o borrador de Internet	Tema	Ubicación
RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*	Describe las características y funciones del protocolo ND (descubrimiento de vecinos) de IPv6	http://www.ietf.org/rfc/rfc2461.txt$number=2461
RFC 3306, *Unicast—Prefix—Based IPv6 Multicast Addresses*	Describe el formato y los tipos de direcciones IPv6 multidifusión	ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt
RFC 3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*	Describe los algoritmos que se usan en la selección de direcciones predeterminadas de IPv6	http://www.ietf.org/rfc/rfc3484?number=3484
RFC 3513, *Internet Protocol version 6 (IPv6) Addressing Architecture*	Contiene información exhaustiva sobre los tipos de direcciones IPv6 con abundantes ejemplos	http://www.ietf.org/rfc/rfc3513.txt?number=3513
RFC 3587, *IPv6 Global Unicast Address Format*	Define el formato estándar de las direcciones IPv6 unidifusión	http://www.ietf.org/rfc/rfc3587.txt?number=3587

7.18 DESCRIPCIÓN GENERAL SOBRE LOS TÚNELES DE IPV6

En la mayoría de las empresas, la implantación de IPv6 en una red IPv4 ya configurada debe realizarse de manera gradual y por fases. El entorno de redes permite el funcionamiento compatible de IPv4 e IPv6. Debido a que casi todas las redes emplean el protocolo IPv4, en la actualidad las redes IPv6 necesitan una forma de comunicarse más allá de sus límites. Para ello, las redes IPv6 se sirven de los túneles.

En buena parte de las situaciones hipotéticas para túneles de IPv6, el paquete de IPv6 saliente se encapsula en un paquete de IPv4. El enrutador de límite de la red IPv6 configura un túnel de extremo a extremo a través de varias redes IPv4 hasta el enrutador de límite de la red IPv6 de destino. El paquete se desplaza por el túnel en dirección al enrutador de límite de la red de destino, que se encarga de

desencapsular el paquete. A continuación, el enrutador reenvía el paquete IPv6 desencapsulado al nodo de destino.

La implementación de IPv6 permite las siguientes situaciones hipotéticas de configuración de túneles:

- Túnel configurado manualmente entre dos redes IPv6, a través de una red IPv4. La red IPv4 puede ser Internet o una red local dentro de una empresa.
- Túnel configurado manualmente entre dos redes IPv4, a través de una red IPv6, en general dentro de una empresa.
- Túnel de 6to4 configurado dinámicamente entre dos redes IPv6, a través de una red IPv4 de una empresa o por Internet.

7.19 SEGURIDAD INTEGRADA EN IPV6 (IPSEC)

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.

Se trata por tanto de algo obligatorio, y no adicional ni “añadido” como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación – “Authentication Header”) y ESP (encriptación – “Encapsulation Security Payload”), que permiten, básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya lo contemplan.

8. GUIA BASICA PARA IMPLEMENTAR IPV6

8.1 PLANIFICACIÓN DE UNA RED IPV6

Implementar IPv6 en una red nueva o ya configurada supone un importante esfuerzo de planificación; es un paso fundamental necesario para conocer una a uno los diferentes componentes de la red y definir estructuradamente el plan de migración adecuado.

Este paso inicial definirá el modelo del plan a seguir, donde se podrá definir el impacto que tendrá la implementación del nuevo modelo, dejando como resultado un cronograma que con certeza mostrara los tiempos necesarios para la realización del proyecto.

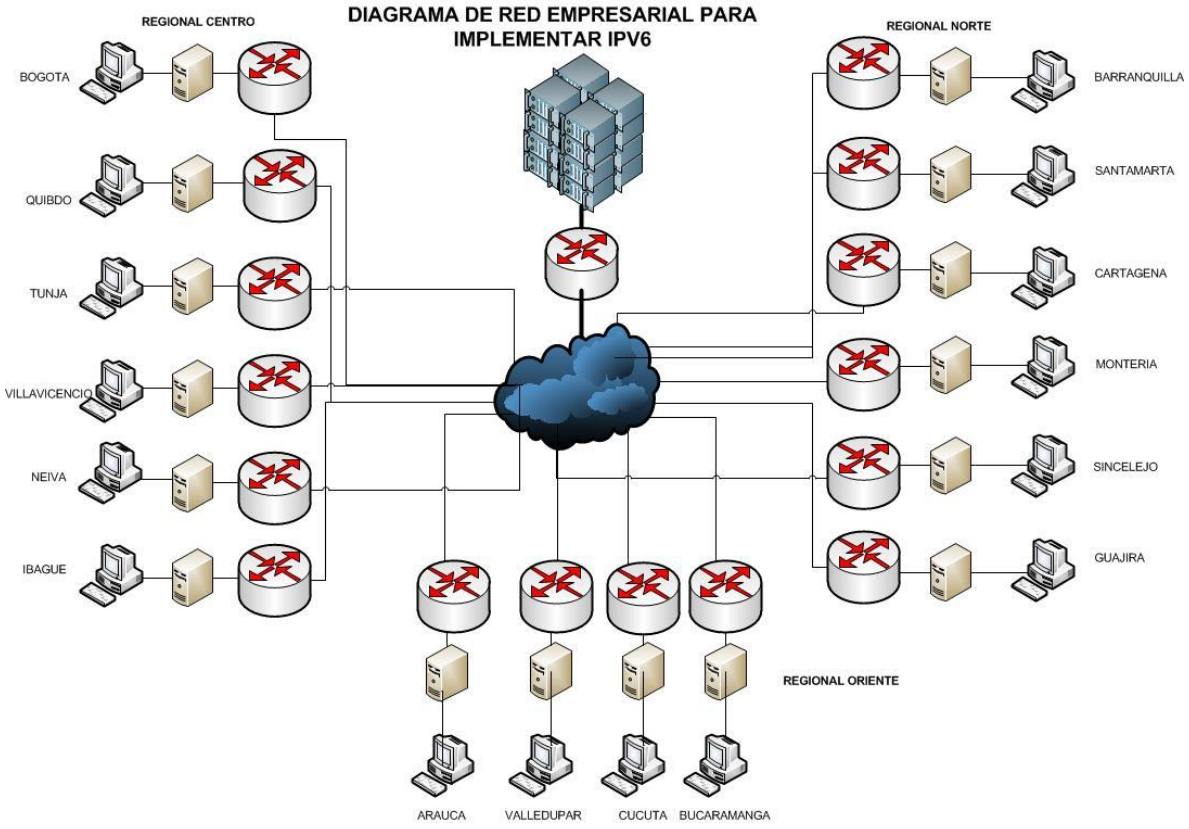
En el caso de redes ya configuradas, la implementación de IPv6 se debe establecer fases, las cuales serán analizadas a profundidad en la planeación inicial de proyecto de migración.

A continuación definimos los pasos básicos necesarios a tener en cuenta en la planeación en redes existentes configuradas en Ipv4.

8.1.1 Mapa de topología física de red. Como primer paso es necesario conocer el escenario donde vamos a trabajar, para ello se debe contar con un mapa físico de la red, donde gráficamente se pueda observar el tipo de dispositivos físicos interconectados (routers, switch, servidores, firewall, host), cabe resaltar que este mapa debe contener toda la red ya que consideramos que esta es una asociación de diferentes redes lan que se comunican a través de túneles, considerando redes de mediano tamaño

Con este diseño queremos ilustrar un caso hipotético de una empresa, la cual hace presencia en diferentes ciudades del país, se quiere mostrar cual sería un ejemplo práctico de lo anteriormente descrito.

Figura 3. Ejemplo modelo de red empresarial para implementación de IPV6



8.1.2 Identificación de componentes físico de la topología de red. La siguiente consideración a tener en cuenta, para lo cual el paso anterior juega un papel importante, es la identificación de todos los componentes físicos o hardware de la red, para esto se debe inventariar de forma ordenada la cantidad de equipos (router, switch, firewall, servidores, host), cada dispositivo debe tener claro su marca, referencia y sistema operativo que lo identifica.

8.1.3 Verificación de compatibilidad de hardware. La identificación de componentes físicos de la red, agrupados por tipo de dispositivo nos lleva a realizar un análisis minucioso de la documentación que cada fabricante entrega de los productos, con ello podemos concluir que dispositivos son compatibles para Ipv6, cuales pueden actualizarse su sistema operativos para hacerlos compatibles y cuáles de este inventario deben ser reemplazados ya que su funcionamiento solo es compatible con IPv4 lo que se convierte en un alto riesgo para la implementación del proyecto de migración.

A continuación describiré una serie de equipos del fabricante cisco los cuales son compatibles con IPv6.

8.1.3.1 Routers

Cisco 3900 Series Integrated Services Routers

Cisco 3900 Series Integrated Services Routers (ISR) están diseñados para satisfacer las demandas de las aplicaciones de medianas y grandes oficinas de hoy en día y evolucionar a los servicios basados en la nube. Ofrecen aplicaciones virtualizadas y colaboración altamente segura a través de la más amplia gama de conectividad WAN de alto rendimiento que ofrece servicios simultáneos de hasta 375 Mbps.

Modelos

- Cisco 3945 Integrated Services Router
- Cisco 3945E Integrated Services Router Cisco 3945E
- Cisco 3925 Integrated Services Router Cisco 3925
- Cisco 3925E Integrated Services Router Cisco 3925E

Consideraciones para implementar IPV6

- Habilitar Ipv6 en la red de la empresa de los routers DMVPN. En particular, se requiere un sistema de nombres de dominio (DNS) para administrar las direcciones IPv6.
- Actualizar el hub-and-spoke routers a Cisco IOS ® Software Release 12.4 (20) T o posterior.
- Aplicar DMVPN para configuraciones de IPv6 en los routers hub-and-spoke.
- Habilitar IPv6 en dispositivos host detrás de los routers spoke.
- La conexión WAN entre los routers hub-and-spoke es sólo IPv4. Routers intermedios no tienen la capacidad de IPv6.
- Debido a que la mayoría de los sitios web y servidores DNS siguen utilizando las direcciones IPv4, es obligatorio contar con direcciones IPv4 e IPv6 en los dispositivos de acogida tras el router spoke para la conectividad con todos los sitios web.
- Por el lado de la LAN, utilice la configuración automática sin estado IPv6 (RFC 2462), que requiere un prefijo de red de 64 bits. Utilice la configuración automática sin estado de todos los dispositivos detrás del router hub-and-spoke para evitar la asignación manual de direcciones IPv6 y para permitir una fácil transición de IPv4 a IPv6.
- IPv6 se admite en Puente Virtual Interface Group (BVI), sólo en otra imagen del software Cisco IOS 15.1 (2) o T1[1].

Cisco 3800 Series Integrated Services Routers

Cisco 3800, es un dispositivo ideal para medianas y grandes empresas, el cual les permiten simplificar la complejidad de la red y soporte de misión crítica de aplicaciones de negocio, por que proporciona una plataforma altamente segura

[1] Disponible EN: http://www.cisco.com/en/US/products/ps10536/index.html

con concurrente T3/E3 garantizando entregas confiables de velocidad de cable de datos, voz, video

Modelos

- Cisco 3845 Integrated services routers
- Cisco 3825 Integrated services routers

Consideraciones para implementar Ipv6

Este modelo de router cisco no son compatibles 100% con IPv6, encontramos grandes falencias en la implementación de varias características necesarias y prioritarias en la transmisión de datos a través de una red las cuales son funcionales en IPv4, pero en su mayoría generan conflictos para implementar un direccionamiento en IPv6.

Características de enrutamiento no compatibles IPv6 Unicast[2]

- Enrutamiento IPv6 basada en políticas
- IPv6 de red privada virtual (VPN) de enrutamiento y reenvío (VRF)
- Paquetes IPv6 destinados a direcciones locales de sitio
- Protocolos de túnel, como IPv4 a IPv6 o IPv6 a IPv4
- El switch como punto final del túnel apoyar protocolos de túnel IPv4 a IPv6 o IPv6 a IPv4
- IPv6 unicast reenvío de ruta inversa
- Prefijos IPv6 generales
- HSRP para IPv6
- SNMP y Syslog a través de IPv6
- MPLS para IPv6
- ACL para IPv6
- BFD para IPv6

[2] Disponible en: http://www.cisco.com/en/US/products/ps5855/index.html

- VRF y VRF-lite para IPv6
- IPv6 Multicast
- RIP para IPv6
- EIGRP IPv6

Cisco 2900 Series Integrated Services Routers

Cisco 2900 series integrated services routers (ISR) están diseñados para satisfacer las demandas de las ramas de tamaño medio de hoy en dia y evolucionar a los servicios basados en la nube.

Ofrecen aplicaciones virtualizadas y colaboración altamente segura a través de la más amplia gama de conectividad WAN de alto rendimiento que ofrece servicios simultáneos de hasta 75 Mbps.

Ofrecen aceleración de cifrado de hardware integrado, procesador con capacidad de señal de video digital (DSP), firewall opcional, detección de prevención de intrusos, procesamiento de llamadas, correo de voz y servicios de aplicaciones.
Además, las plataformas de apoyo de las industrias más amplia gama de opciones de conectividad por cable e inalámbricas, tales como T1/E1, T3/E3, xDSL, cobre y fibra de GE.

Modelos

- Cisco 2921 Integrated Services Router
- Cisco 2921 Integrated Services Router
- Cisco 2911 Integrated Services Router
- Cisco 2901 Integrated Services Router

Consideraciones para implementar Ipv6

Este modelo de routers es el más conocido en la mediana empresa ya que su costo es favorable al consumidor apoyado en sus variables características de funcionalidad, lo que lo ha convertido en un modelo con innumerables condiciones de uso, haciendo parte de la gran mayoría de centro de datos.

Este modelo es compatible con protocolos como Eigrp, Ospf y Rip permitiendo su implementación y configuración en Ipv6, garantizando seguridad, confiabilidad e integridad en la transmisión de los datos a través de la red.
ttp://www.cisco.com/en/US/products/ps10537/index.html

8.1.3.2 Switches

Switches Cisco Nexus de la serie 7000

Para los centros de datos, la serie 7000 de Cisco Nexus ofrece una solución de extremo a extremo en una sola plataforma para el núcleo de datos, agregación y conectividad de servidor de extremo de la fila y parte superior del bastidor de alta densidad. Para implementaciones de núcleo de campus, proporciona una solución escalable, con gran capacidad de recuperación y de alto rendimiento.

La plataforma Cisco Nexus de la serie 7000 se ejecuta en el software Cisco NX-OS. Se diseñó específicamente para las implementaciones más críticas en el centro de datos y el campus.

Modelos

- Switch Cisco Nexus 7000 de 18 ranuras
- Switch Cisco Nexus 7000 de 10 ranuras
- Switch Cisco Nexus 7000 de 9 ranuras

IPv6 tiene los siguientes requisitos previos:

- Usted debe estar familiarizado con los conceptos básicos de IPv6 como direcciones IPv6, la información de cabecera IPv6, ICMPv6, y el Protocolo IPv6 Neighbor Discovery (ND).
- Asegúrese de seguir las pautas de memoria / procesamiento al realizar un dispositivo de un dispositivo de doble pila (IPv4/IPv6).

IPv6 tiene las siguientes pautas para la configuración y limitaciones:

- Paquetes IPv6 son transparentes para los switches de Capa 2 LAN debido a que los switches no examinan Layer 3 información del paquete antes de reenviar tramas IPv6. Hosts IPv6 se puede conectar directamente a la capa 2 switches LAN.
- Puede configurar varias direcciones IPv6 globales dentro del mismo prefijo en una interfaz. Sin embargo, no se admiten varias direcciones locales de vínculo IPv6 en una interfaz.
- Debido RFC 3879 desaprueba el uso de direcciones locales de sitio, debe configurar las direcciones IPv6 privados según las recomendaciones del local único direccionamiento (ULA) en el RFC 4193.

Cisco Catalyst 5000 Series Swiches

Cisco Catalyst familia de la serie 5000 ofrece una Ethernet Gigabit y ATM listos ofreciendo a los usuarios la plataforma de tecnologías de concentración de enlaces de alta velocidad, incluyendo Fast EthernetChannel.

La serie Catalyst 5000 también cuenta con una arquitectura redundante, VLANs dinámicas, soporte completo servicios de intranet, y el rendimiento medio de cambio con una amplia variedad de módulos de interfaz. Módulos para el chasis de la familia Catalyst 5000 - Catalyst 5500, 5509, 5505, 5000 y 5002 - se han diseñado para una completa interoperabilidad y protección

de la inversión. Catalizador de la familia 5000 es compatible con NetFlow multiprotocolo de conmutación para la convergencia escalable de Layer 2 y Layer 3, conmutación añadiendo los beneficios de multiprotocolo de conmutación multicapa y otros servicios de red de Cisco IOS.

Modelos

- Cisco catalyst 5000
- Cisco catalyst 5002

Este modelo de swich es compatible con IPv4, IPv6, soportando las diferentes aplicaciones y protocolos de comunicación, soportando direccionamientos y filtrados de seguridad con ACL[3].

Cisco Industrial Ethernet 2000 (IE 2000) Series Switches

Cisco Industrial Ethernet 2000 (IE 2000) Series Switches extienden las tecnologías Cisco Catalyst probados prevalentes en las redes empresariales para redes industriales se extienden así la seguridad superior, video y servicios de voz de la empresa a las aplicaciones industriales. También son robustos, fáciles de manejar, resistente, y mejorado a través de protocolos específicos de la industria.

Características

- Seguridad superior, con funciones completas, como IEEE 802.1x, SSH, snooping DHCP, y el control de tormentas
- Protocolos industriales específicos, como IEEE1588, CIP, y PROFINET
- La facilidad de manejo, con el Administrador de dispositivos, Asistente de red Cisco, Cisco Prime, y soluciones de administración de terceros

[3] Disponible en: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/sec_ipacls.html

- La resiliencia y la recuperación de red rápida con Flex Links, y la convergencia rápida con Protocolo Ethernet Resilient Cisco (REP)
- Simplificado de gestión de direcciones IP y el despliegue, con la traducción de direcciones de red (NAT).

Encontramos que esta serie de swich son compatibles con los protocolos Ipv4 e Ipv6, los cuales son funciónales en los dos direccionamientos y entre ellos[4].

Cisco IGX 8400 Label Swich Router

Tecnología de conmutación de etiquetas multiprotocolo basada en estándares (MPLS) está disponible en la plataforma Series IGX conmutador multiservicio Cisco 8400. Un punto de entrada a MPLS en una plataforma de clase portadora, el Cisco IGX 8400 amplía el alcance del éxito de la tecnología MPLS BPX 8600, a menudo se utiliza junto con el Cisco IGX.

El Cisco IGX 8400 es ideal para correo, teléfono, telégrafo y los transportistas (PTT) y los proveedores alternativos que ofrecen servicios de modo de transferencia asíncrono (ATM), Frame Relay y los puntos medianos o distribuida de presencia (POPs), así como para instalaciones que requieren una solución multiservicio robusto, rentable. El Cisco IGX 8400 trae las ventajas de escalabilidad de IP + ATM a las grandes empresas en todo el mundo.

El Cisco IGX se puede actualizar con funcionalidad IP con la adición de la IGX-LSC-72 Label Switch Controller Kit de modificación. Con el regulador de interruptor Label reequipamiento, la IGX ofrece capacidades líderes en la industria de servicios de banda ancha ATM e integra el software Cisco IOS ® para ofrecer servicios IP. La adición de un IGX-LSC-72 a un IGX permite la ampliación de los

[4] Disponible en: http://www.cisco.com/en/US/prod/collateral/switches/ps9876/ps12451/data_sheet_c78-705523.html

servicios de Internet y permite al usuario prestación nueva IP integrado + cajero tales como voz sobre IP (VoIP), redes privadas virtuales (VPNs), y la web y de alojamiento de contenido servicios a través de la columna vertebral ATM.

Características y beneficios de Cisco IGX 8400 Label Switch Router

El controlador de conmutación de etiquetas (LSC), junto con el Cisco 8400 IP IGX mas conmutador ATM, soporta la integración escalable de servicios IP sobre una red ATM. El MPLS LSC permite Cisco IGX 8400 a:

- Participar en una red MPLS
- Directamente mirar con routers IP
- Apoyar las funciones de IP en el software Cisco IOS

Modelos[5]

- Cisco IGX 8450 SES Multiservice Switch
- Cisco IGX 8400 MPLS Label Switch Router

8.1.3.3 Firewall

Firewall Cisco ASA 5585-X Adaptive Security Appliance

A diferencia de la mayoría de los proveedores de seguridad que le obliguen a elegir entre un servidor de seguridad de alta calidad y un sistema de prevención de intrusos efectiva (IPS), Cisco combina una probada firewall con una única integral del sistema de prevención de intrusiones . Esto hace que el Cisco ASA 5585-X Adaptive Security Appliance una solución de seguridad, eficaz y efectiva. Ofrece ocho veces la densidad de rendimiento de cortafuegos competitivos, con:

- Los conteos más altos de sesión VPN

[5] Disponible en: http://www.cisco.com/en/US/products/hw/switches/ps988/index.html

- El doble de conexiones por segundo
- Cuatro veces la capacidad de conexión

De esta forma, se ajusta a las necesidades crecientes de las organizaciones más dinámicas de hoy - todo en una unidad de rack compacto de dos (2 RU) huella.

La mayoría de los dispositivos de seguridad requieren hasta 16RU y 5100 vatios de escalar al nivel de rendimiento que el ASA 5585-X alcanzan con sólo 2RU y 785 vatios. Además, los IPS integrados con Correlación Global es dos veces más eficaz que los sistemas tradicionales de prevención de intrusiones.

Características y Capacidades[6]

- Reduce los costes de adquisición iniciales en un 80 por ciento
- Reduce los costos de consumo de energía en un 85 por ciento
- Reduce los requisitos de espacio en rack en un 88 por ciento
- Simplifica la integración y la gestión de la red
- Se amplía hasta 80 Gbps (con dos módulos de firewall en un solo chasis)

8.1.3.4 Servidores: Los servidores hacen parte de las lista de equipos activos de una red y es necesario revisar que consideraciones se deben tener en cuenta para implementar IPv6.

Los servidores son considerados equipos de procesamiento normal por lo tanto se debe considerar que las tarjetas de red acepten la configuración del protocolo IPv6 ya que este sería el único impedimento para que el equipo fuese aceptado dentro de un direccionamiento IPv6.

[6] Disponible en: http://www.cisco.com/en/US/products/ps11061/index.html

Sin embargo encontramos que los servidores son elementos fundamentales en el contexto de la red, ya que sobre estos dispositivos se implementa diferentes servicios y aplicaciones.

En este caso particular tendremos en cuenta servicios como HTTP, NFS, DNS, FTP, los cuales serán evaluados y diagnosticados aportando una ayuda para el momento de implementar un direccionamiento IPv6.

8.1.4 Solicitud de prefijos IPv6. El diagrama del mapa físico no solo nos debe mostrar los componentes físicos, sino también los diferentes enlaces utilizados para interconectar las diferentes subredes entre sí, para ello es necesario la identificación de cuantas direcciones con prefijo 48 debemos solicitar, en IPv4 utilizamos direcciones públicas las cuales serán reemplazadas por prefijo IPv6.

Es importante que los proveedores de servicios cuenten con este mecanismo de asignación de direcciones IPv6, ya que son ellos los principales actores de intercomunicación y deben garantizar la disponibilidad del servicio en IPv6.

Se debe evaluar que el proveedor de servicios adicional a poder entregar las direcciones en prefijo 48, también cuente con la cobertura y la tecnología en todas las ciudades que necesitamos interconectar, de lo contrario sería un tropiezo en la migración e implementación de IPv6.

8.1.5 Elaboración de tablas de direccionamiento IPv6. Las tablas de direccionamiento son pilar importante en la migración a la nueva tecnología, hay que tener claro que este direccionamiento opera desde la parte de enrutadores hasta los host, y a través de diferentes protocolos son entregados a los diferentes componentes de la red.

En el caso de los routers y swiches utilizan protocolos como ospf, eigrp o rip para enlazar estos dispositivos y entregar las tablas de direccionamiento, las cuales hacen posible la comunicación entre las diferentes subredes de la red.

Para ello es necesario tener claro que antes de realizar cualquier configuración se debe elaborar estas tablas, donde se documente la topología de direcciones de la red.

La tabla siguiente muestra un ejemplo de la asignación de prefijos de IPv4 privados a prefijos de IPv6.

Tabla 5. Creación de un esquema de numeración para subredes

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

A continuación ilustraremos un ejemplo de una tabla de direccionamiento en IPv6, diseñada para el modelo tomado como ejemplo en la migración a Ipv6.

Tabla 6. Regional centro

REGIONAL CENTRO																		
ID	BOGOTA			QUIBDO			TUNJA			VILLAVICENCIO			NEIVA			IBAGUE		
	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST
1	2801::1C00	0001	:::0001	2801::1C00	0002	:::0001	2801::1C00	0003	:::0001	2801::1C00	0004	:::0001	2801::1C00	0005	:::0001	2801::1C00	0006	:::0001
2	2801::1C00	0001	:::0002	2801::1C00	0002	:::0002	2801::1C00	0003	:::0002	2801::1C00	0004	:::0002	2801::1C00	0005	:::0002	2801::1C00	0006	:::0002
3	2801::1C00	0001	:::0003	2801::1C00	0002	:::0003	2801::1C00	0003	:::0003	2801::1C00	0004	:::0003	2801::1C00	0005	:::0003	2801::1C00	0006	:::0003
4	2801::1C00	0001	:::0004	2801::1C00	0002	:::0004	2801::1C00	0003	:::0004	2801::1C00	0004	:::0004	2801::1C00	0005	:::0004	2801::1C00	0006	:::0004
5	2801::1C00	0001	:::0005	2801::1C00	0002	:::0005	2801::1C00	0003	:::0005	2801::1C00	0004	:::0005	2801::1C00	0005	:::0005	2801::1C00	0006	:::0005
6	2801::1C00	0001	:::0006	2801::1C00	0002	:::0006	2801::1C00	0003	:::0006	2801::1C00	0004	:::0006	2801::1C00	0005	:::0006	2801::1C00	0006	:::0006
7	2801::1C00	0001	:::0007	2801::1C00	0002	:::0007	2801::1C00	0003	:::0007	2801::1C00	0004	:::0007	2801::1C00	0005	:::0007	2801::1C00	0006	:::0007
8	2801::1C00	0001	:::0008	2801::1C00	0002	:::0008	2801::1C00	0003	:::0008	2801::1C00	0004	:::0008	2801::1C00	0005	:::0008	2801::1C00	0006	:::0008
9	2801::1C00	0001	:::0009	2801::1C00	0002	:::0009	2801::1C00	0003	:::0009	2801::1C00	0004	:::0009	2801::1C00	0005	:::0009	2801::1C00	0006	:::0009
10	2801::1C00	0001	:::0010	2801::1C00	0002	:::0010	2801::1C00	0003	:::0010	2801::1C00	0004	:::0010	2801::1C00	0005	:::0010	2801::1C00	0006	:::0010
11	2801::1C00	0001	:::0011				2801::1C00	0003	:::0011	2801::1C00	0004	:::0011	2801::1C00	0005	:::0011	2801::1C00	0006	:::0011
12	2801::1C00	0001	:::0012				2801::1C00	0003	:::0012	2801::1C00	0004	:::0012	2801::1C00	0005	:::0012	2801::1C00	0006	:::0012
13	2801::1C00	0001	:::0013				2801::1C00	0003	:::0013	2801::1C00	0004	:::0013	2801::1C00	0005	:::0013	2801::1C00	0006	:::0013
14	2801::1C00	0001	:::0014				2801::1C00	0003	:::0014	2801::1C00	0004	:::0014	2801::1C00	0005	:::0014	2801::1C00	0006	:::0014
15	2801::1C00	0001	:::0015				2801::1C00	0003	:::0015	2801::1C00	0004	:::0015	2801::1C00	0005	:::0015	2801::1C00	0006	:::0015
16	2801::1C00	0001	:::0016				2801::1C00	0003	:::0016	2801::1C00	0004	:::0016				2801::1C00	0006	:::0016
17	2801::1C00	0001	:::0017				2801::1C00	0003	:::0017	2801::1C00	0004	:::0017				2801::1C00	0006	:::0017
18	2801::1C00	0001	:::0018				2801::1C00	0003	:::0018	2801::1C00	0004	:::0018				2801::1C00	0006	:::0018
19	2801::1C00	0001	:::0019				2801::1C00	0003	:::0019									
20	2801::1C00	0001	:::0020				2801::1C00	0003	:::0020									
21	2801::1C00	0001	:::0021				2801::1C00	0003	:::0021									
22							2801::1C00	0003	:::0022									
23							2801::1C00	0003	:::0023									
24							2801::1C00	0003	:::0024									
25							2801::1C00	0003	:::0025									
26							2801::1C00	0003	:::0026									

Tabla 7. Regional Norte

REGIONAL NORTE																		
ID	BARRANQUILLA			SANTAMARTA			CARTAGENA			MONTERIA			SINCELEJO			GUIAJIRA		
	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST
1	2801::1C00	0007	:::0001	2801::1C00	0008	:::0001	2801::1C00	0009	:::0001	2801::1C00	0010	:::0001	2801::1C00	0011	:::0001	2801::1C00	0012	:::0001
2	2801::1C00	0007	:::0002	2801::1C00	0008	:::0002	2801::1C00	0009	:::0002	2801::1C00	0010	:::0002	2801::1C00	0011	:::0002	2801::1C00	0012	:::0002
3	2801::1C00	0007	:::0003	2801::1C00	0008	:::0003	2801::1C00	0009	:::0003	2801::1C00	0010	:::0003	2801::1C00	0011	:::0003	2801::1C00	0012	:::0003
4	2801::1C00	0007	:::0004	2801::1C00	0008	:::0004	2801::1C00	0009	:::0004	2801::1C00	0010	:::0004	2801::1C00	0011	:::0004	2801::1C00	0012	:::0004
5	2801::1C00	0007	:::0005	2801::1C00	0008	:::0005	2801::1C00	0009	:::0005	2801::1C00	0010	:::0005	2801::1C00	0011	:::0005	2801::1C00	0012	:::0005
6	2801::1C00	0007	:::0006	2801::1C00	0008	:::0006	2801::1C00	0009	:::0006	2801::1C00	0010	:::0006	2801::1C00	0011	:::0006	2801::1C00	0012	:::0006
7	2801::1C00	0007	:::0007	2801::1C00	0008	:::0007	2801::1C00	0009	:::0007	2801::1C00	0010	:::0007	2801::1C00	0011	:::0007	2801::1C00	0012	:::0007
8	2801::1C00	0007	:::0008	2801::1C00	0008	:::0008	2801::1C00	0009	:::0008	2801::1C00	0010	:::0008	2801::1C00	0011	:::0008	2801::1C00	0012	:::0008
9	2801::1C00	0007	:::0009	2801::1C00	0008	:::0009	2801::1C00	0009	:::0009	2801::1C00	0010	:::0009	2801::1C00	0011	:::0009	2801::1C00	0012	:::0009
10	2801::1C00	0007	:::0010	2801::1C00	0008	:::0010	2801::1C00	0009	:::0010	2801::1C00	0010	:::0010	2801::1C00	0011	:::0010	2801::1C00	0012	:::0010
11	2801::1C00	0007	:::0011	2801::1C00	0008		2801::1C00	0009	:::0011	2801::1C00	0010	:::0011	2801::1C00	0011	:::0011	2801::1C00	0012	:::0011
12	2801::1C00	0007	:::0012	2801::1C00	0008		2801::1C00	0009	:::0012	2801::1C00	0010	:::0012	2801::1C00	0011	:::0012	2801::1C00	0012	:::0012
13	2801::1C00	0007	:::0013	2801::1C00	0008		2801::1C00	0009	:::0013	2801::1C00	0010	:::0013	2801::1C00	0011	:::0013	2801::1C00	0012	:::0013
14	2801::1C00	0007	:::0014	2801::1C00	0008		2801::1C00	0009	:::0014	2801::1C00	0010	:::0014	2801::1C00	0011	:::0014			
15	2801::1C00	0007	:::0015	2801::1C00	0008		2801::1C00	0009	:::0015	2801::1C00	0010	:::0015	2801::1C00	0011	:::0015			
16	2801::1C00	0007	:::0016	2801::1C00	0008		2801::1C00	0009	:::0016	2801::1C00	0010	:::0016	2801::1C00	0011	:::0016			
17	2801::1C00	0007	:::0017	2801::1C00	0008		2801::1C00	0009	:::0017	2801::1C00	0010	:::0017						
18	2801::1C00	0007	:::0018	2801::1C00	0008		2801::1C00	0009	:::0018	2801::1C00	0010	:::0018						
19	2801::1C00	0007	:::0019	2801::1C00	0008		2801::1C00	0009	:::0019									
20	2801::1C00	0007	:::0020				2801::1C00	0009	:::0020									
21	2801::1C00	0007	:::0021				2801::1C00	0009	:::0021									
22	2801::1C00	0007	:::0022				2801::1C00	0009	:::0022									
23	2801::1C00	0007	:::0023				2801::1C00	0009	:::0023									
24	2801::1C00	0007	:::0024				2801::1C00	0009	:::0024									
25	2801::1C00	0007	:::0025				2801::1C00	0009	:::0025									
26	2801::1C00	0007	:::0026				2801::1C00	0009	:::0026									
27	2801::1C00	0007	:::0027				2801::1C00	0009	:::0027									
28	2801::1C00	0007	:::0028				2801::1C00	0009	:::0028									
29	2801::1C00	0007	:::0029				2801::1C00	0009	:::0029									
30	2801::1C00	0007	:::0030				2801::1C00	0009	:::0030									

Tabla 8. Regional Oriente

REGIONAL ORIENTE												
ID	ARAUCA			VALLEDUPAR			NORTE DE SANTANDER			SANTANDER		
	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST	RED	SUBRED	HOST
1	2801::1C00	0013	:::0001	2801::1C00	0017	:::0001	2801::1C00	0018	:::0001	2801::1C00	0019	:::0001
2	2801::1C00	0013	:::0002	2801::1C00	0017	:::0002	2801::1C00	0018	:::0002	2801::1C00	0019	:::0002
3	2801::1C00	0013	:::0003	2801::1C00	0017	:::0003	2801::1C00	0018	:::0003	2801::1C00	0019	:::0003
4	2801::1C00	0013	:::0004	2801::1C00	0017	:::0004	2801::1C00	0018	:::0004	2801::1C00	0019	:::0004
5	2801::1C00	0013	:::0005	2801::1C00	0017	:::0005	2801::1C00	0018	:::0005	2801::1C00	0019	:::0005
6	2801::1C00	0013	:::0006	2801::1C00	0017	:::0006	2801::1C00	0018	:::0006	2801::1C00	0019	:::0006
7	2801::1C00	0013	:::0007	2801::1C00	0017	:::0007	2801::1C00	0018	:::0007	2801::1C00	0019	:::0007
8	2801::1C00	0013	:::0008	2801::1C00	0017	:::0008	2801::1C00	0018	:::0008	2801::1C00	0019	:::0008
9	2801::1C00	0013	:::0009	2801::1C00	0017	:::0009	2801::1C00	0018	:::0009	2801::1C00	0019	:::0009
10	2801::1C00	0013	:::0010	2801::1C00	0017	:::0010	2801::1C00	0018	:::0010	2801::1C00	0019	:::0010
11	2801::1C00	0013	:::0011				2801::1C00	0018	:::0011	2801::1C00	0019	:::0011
12	2801::1C00	0013	:::0012				2801::1C00	0018	:::0012	2801::1C00	0019	:::0012
13	2801::1C00	0013	:::0013				2801::1C00	0018	:::0013	2801::1C00	0019	:::0013
14							2801::1C00	0018	:::0014	2801::1C00	0019	:::0014
15							2801::1C00	0018	:::0015	2801::1C00	0019	:::0015
16							2801::1C00	0018	:::0016	2801::1C00	0019	:::0016
17										2801::1C00	0019	:::0017
18										2801::1C00	0019	:::0018
19										2801::1C00	0019	:::0019
20										2801::1C00	0019	:::0020
21										2801::1C00	0019	:::0021
22										2801::1C00	0019	:::0022
23										2801::1C00	0019	:::0023
24										2801::1C00	0019	:::0024
25										2801::1C00	0019	:::0025
26										2801::1C00	0019	:::0026
27										2801::1C00	0019	:::0027
28										2801::1C00	0019	:::0028
29										2801::1C00	0019	:::0029
30										2801::1C00	0019	:::0030
31										2801::1C00	0019	:::0031
32										2801::1C00	0019	:::0032
33										2801::1C00	0019	:::0033
34										2801::1C00	0019	:::0034
35										2801::1C00	0019	:::0035
36										2801::1C00	0019	:::0036
37										2801::1C00	0019	:::0037
38										2801::1C00	0019	:::0038
39										2801::1C00	0019	:::0039
40										2801::1C00	0019	:::0040
41										2801::1C00	0019	:::0041
42										2801::1C00	0019	:::0042
43										2801::1C00	0019	:::0043
44										2801::1C00	0019	:::0044
45										2801::1C00	0019	:::0045
46										2801::1C00	0019	:::0046
47										2801::1C00	0019	:::0047

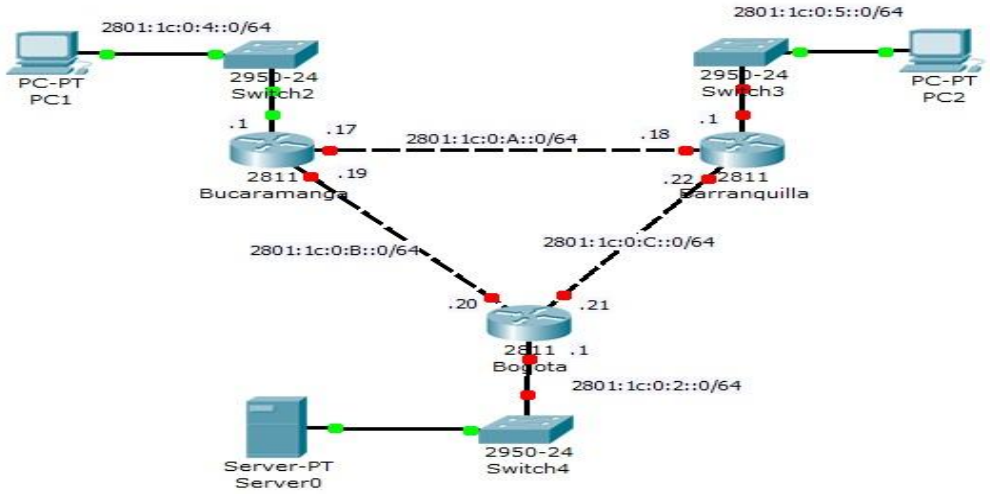
8.1.6 Simulación para implementar IPV6 OSPF, EIGRP y RIP en Packet Tracer

- **Objetivo:** En esta práctica buscamos definir los pasos a seguir para la implementación de IPv6 en un modelo de red, para ello definimos un esquema básico de una topología de red y a través de packer tracer realizaremos la práctica de implementación, documentando todos los comandos y sentencias ejecutadas necesarias en la implementación de los protocolos OSPF, EIGRP y RIP.

➢ DESARROLLO DE LA SIMULACIÓN

1. Como primer paso se define la siguiente topología de red para implementar IPv6.

Figura 4. Topología de red simulación IPV6



2. Definición de tabla de direccionamiento.

Tabla 9. Direccionamiento IPv6 topología de red

Dispositivo	FasEthernet	IP Address
R1 Bucaramanga	F 1/1	2801:1C:0:4::1/64
	F 1/0	2801:1C:0:B::19/64
	F 0/1	2801:1C:0:A::17/64
R2 Barranquilla	F 1/0	2801:1C:0:C::22/64
	F 0/0	2801:1C:0:A::18/64
	F 1/1	2801:1C:0:5::1/64
R3 Bogotá	F 1/0	2801:1C:0:2::1/64
	F 0/0	2801:1C:0:B::20/64
	F 1/1	2801:1C:0:C::21/64

3. Ejecutamos la aplicación de PACKET TRACER, e ingresamos a cada uno de los dispositivos de red definidos en el modelo, iniciando la configuración de cada uno de ellos, utilizamos esta técnica de configurar primero cada uno de ellos buscando utilizar la misma topología en la implementación de OSPF, EIGRP y RIP.
4. Iniciamos definiendo los nombres a los 3 routers definidos en el modelo.

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Bucaramanga
```

Nota1: Este paso se debe repetir en los routers restantes.

5. Configurar en cada router el encaminamiento de paquetes IPv6

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

6. Configurar IPv6 en las Interfaz FastEthernet.

```
Bucaramanga>enable
Bucaramanga#configure terminal
Bucaramanga(config)#int f1/1
Bucaramanga(config-if)#ipv6 enable
Bucaramanga(config-if)#ipv6 address 2801:1c:0:4::1/64
Bucaramanga(config-if)#no shutdown
Bucaramanga(config-if)#exit
```

Nota2: Se repite el paso anterior para configurar cada Interfaz FasEthernet en cada Router, según la tabla de direccionamiento.

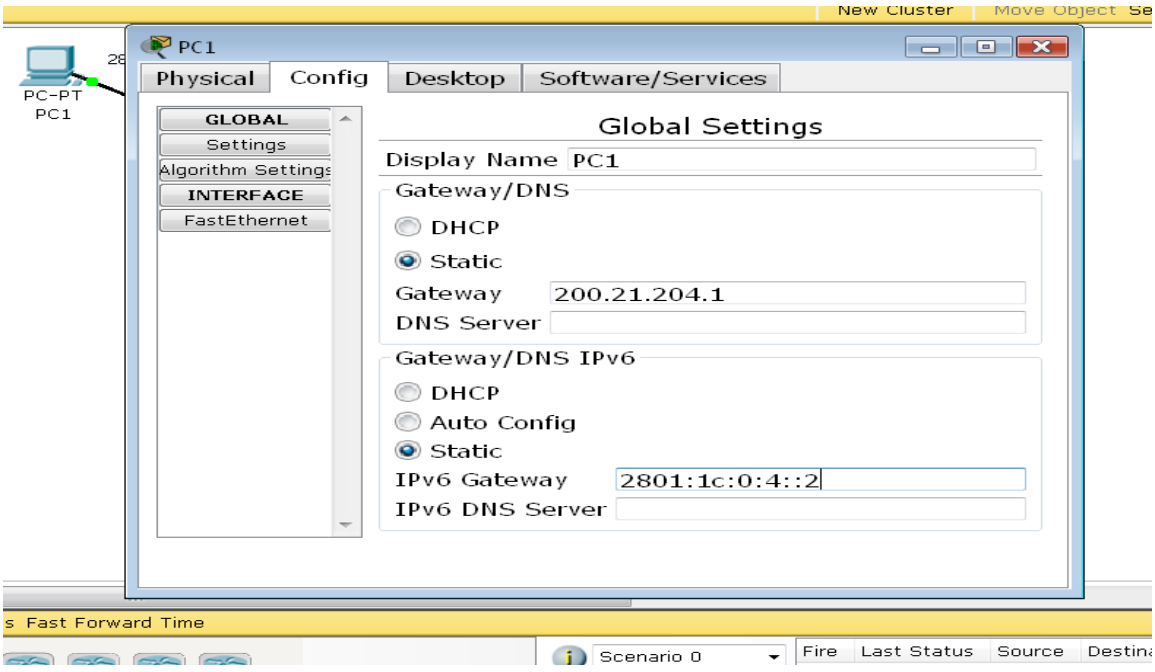
7. Se realiza una prueba de conexión entre routers directamente conectados.

```
Bucaramanga#ping 2801:1c:0:A::18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2801:1c:0:A::18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/16/45 ms
```

8. Asignación de ipv6 al host.

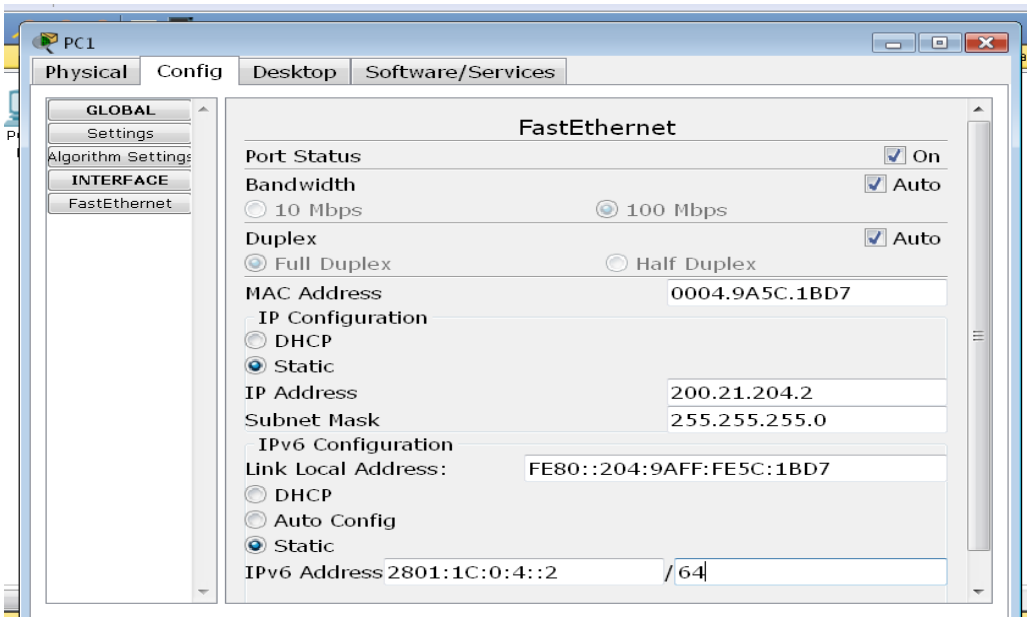
Una vez se configuren los routers, se configuran las IP de cada equipo, se debe ingresar a la pestaña “config” y en la opción “Settings” dentro del apartado “GLOBAL” se activara la casilla de “Static” y en el cuadro de texto “IPv6 Gateway” se deberá asignar la dirección quedando se la siguiente manera:

Figura 5. Asignación de IPV6 host



Ahora se debe ir “INTERFACE” en el iten de “FastEhernet”, se observa que dentro del recuadro “IPv6 Configuration” la casilla de “Static” se deberá colocar la dirección ipv6.

Figura 6. Configuración de IPV6



Nota 3: Este proceso se debe realizar en cada host.

➢ CONFIGURACIÓN DE DIRECCIONAMIENTO OSPF

A continuación se procede hacer la implementación de OSPF en la topología definida, documentando los comandos utilizados.

Bucaramanga>enable
Bucaramanga#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#ipv6 unicast-routing
Bucaramanga(config)#ipv6 router ospf 100

%OSPFv3-4-NORTRID: OSPFv3 process 100 could not pick a router-id,please configure manually
Bucaramanga(config-rtr)#router-id 1.1.1.1
Bucaramanga(config-rtr)#exit

Luego se configura cada Interfaz FastEthernet en cada router.

Bucaramanga(config)#int f1/1
Bucaramanga(config-if)#ipv6 add 2801:1c:0:4::1/64
Bucaramanga(config-if)#ipv6 ospf 100 area 0
Bucaramanga(config-if)#no sh
Bucaramanga(config-if)#exit

- **DOCUMENTACION DEL PROCEDIMIENTO REALIZADO**

CONFIGURACION OSPF BUCARAMANGA

Bucaramanga>enable
Bucaramanga#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
Bucaramanga(config-rtr)#router-id 1.1.1.1
Bucaramanga(config-rtr)#exit
Bucaramanga(config)#int f0/1
Bucaramanga(config-if)#ipv6 ospf 1 area 0
Bucaramanga(config-if)#no sh
Bucaramanga(config-if)#exit
Bucaramanga(config)#int f1/0
Bucaramanga(config-if)#ipv6 ospf 1 area 0

Bucaramanga(config-if)#no sh
Bucaramanga(config-if)#exit
Bucaramanga(config)#
Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console

CONFIGURACION OSPF BARRANQUILLA

Barranquilla>ENABLE
Barranquilla#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Barranquilla(config)#ipv6 router ospf 2
%OSPFv3-4-NORTRID: OSPFv3 process 2 could not pick a router-id,please configure manually
Barranquilla(config-rtr)#router-id 1.1.1.2
Barranquilla(config-rtr)#exit
Barranquilla(config)#int f 0/0
Barranquilla(config-if)#ipv6 ospf 2 area 0
Barranquilla(config-if)#no sh
Barranquilla(config-if)#int f 1/0
Barranquilla(config-if)#ipv6 ospf 2 area 0
Barranquilla(config-if)#no sh
Barranquilla(config-if)#exit
Barranquilla(config)#

CONFIGURACION OSPF BOGOTA

Bogota>enable
Bogota#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ipv6 router ospf 3

%OSPFv3-4-NORTRID: OSPFv3 process 3 could not pick a router-id,please configure manually

Bogota(config-rtr)#router-id 1.1.1.3

Bogota(config-rtr)#exit

Bogota(config)#int f0/0

Bogota(config-if)#ipv6 ospf 3 area 0

Bogota(config-if)#no sh

Bogota(config-if)#exit

Bogota(config)#int f 0/1

Bogota(config-if)#ipv6 ospf 3 area 0

Bogota(config-if)#no sh

Bogota(config-if)#exit

Bogota(config)#

- **CONFIGURACIÓN DE DIRECCIONAMIENTO EIGRP**

CONFIGURACION EIGRP BUCARAMANGA

Bucaramanga>enable

Bucaramanga#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

Bucaramanga(config)#ipv6 unicast-routing

Bucaramanga(config)#int f0/1

Bucaramanga(config-if)#ipv6 eigrp 100

Bucaramanga(config-if)#exit

Bucaramanga(config)#ipv6 router eigrp 100

Bucaramanga(config-rtr)#router-id 10.1.1.5

Bucaramanga(config-rtr)#no sh

Bucaramanga(config-rtr)#exit

Bucaramanga(config)#ipv6 unicast-routing
Bucaramanga(config)#int f1/0
Bucaramanga(config-if)#ipv6 add 2801:1c:0:b::19/64
Bucaramanga(config-if)#ipv6 eigrp 100
Bucaramanga(config-if)#exit
Bucaramanga(config)#int f0/1
Bucaramanga(config-if)#ipv6 add 2801:1c:0:A::17/64
Bucaramanga(config-if)#ipv6 eigrp 100
Bucaramanga(config-if)#exit
Bucaramanga(config)#int f1/1
Bucaramanga(config-if)#ipv6 add 2801:1c:0:4::1/64
Bucaramanga(config-if)#ipv6 eigrp 100
Bucaramanga(config-if)#exit

CONFIGURACION EIGRP BARRANQUILLA

Barranquilla>ENABLE
Barranquilla#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Barranquilla(config)#ipv6 router eigrp 100
Barranquilla(config-rtr)#router-id 10.1.1.4
Barranquilla(config-rtr)#no sh
Barranquilla(config-rtr)#exit
Barranquilla(config)#int f 0/0
Barranquilla(config-if)#ipv6 add 2801:1c:0:A::18/64
Barranquilla(config-if)#ipv6 eigrp 100
Barranquilla(config-if)#exit
Barranquilla(config)#int f 1/0
Barranquilla(config-if)#ipv6 add 2801:1c:0:C::22/64
Barranquilla(config-if)#ipv6 eigrp 100
Barranquilla(config-if)#exit

Barranquilla(config)#int f1/1

Barranquilla(config-if)#ipv6 add 2801:1c:0:5::1/64

Barranquilla(config-if)#ipv6 eigrp 100

Barranquilla(config-if)#exit

CONFIGURACION EIGRP BOGOTA

Bogota>enable

Bogota#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

Bogota(config)#ipv6 router eigrp 100

Bogota(config-rtr)#router-id 10.1.1.2

Bogota(config-rtr)#no sh

Bogota(config-rtr)#exit

Bogota(config)#int f0/0

Bogota(config-if)#ipv6 add 2801:1c:0:B::20/64

Bogota(config-if)#ipv6 eigrp 100

Bogota(config-if)#exit

Bogota(config)#int f0/1

Bogota(config-if)#ipv6 add 2801:1c:0:C::21/64

Bogota(config-if)#ipv6 eigrp 100

Bogota(config-if)#exit

Bogota(config)# int f 1/0

Bogota(config-if)#ipv6 add 2801:1c:0:2::1/64

Bogota(config-if)#ipv6 eigrp 100

Bogota(config-if)#exit

- **CONFIGURACIÓN DE DIRECCIONAMIENTO RIP**

CONFIGURACION RIP BUCARAMANGA

Bucaramanga>enable

Bucaramanga#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Bucaramanga(config)#ipv6 unicast-routing

Bucaramanga(config)#ipv6 router rip simulacion

Bucaramanga(config-rtr)#exit

Bucaramanga(config)#int f0/1

Bucaramanga(config-if)#ipv6 rip simulacion enable

Bucaramanga(config-if)#exit

Bucaramanga(config)#int f1/0

Bucaramanga(config-if)#ipv6 rip simulacion enable

Bucaramanga(config-if)#exit

Bucaramanga(config)#int f1/1

Bucaramanga(config-if)#ipv6 rip simulacion enable

Bucaramanga(config-if)#exit

CONFIGURACION RIP BARRANQUILLA

Barranquilla>ENABLE

Barranquilla#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

Barranquilla(config)#ipv6 unicast-routing

Barranquilla(config)#ipv6 router rip simulacion

Barranquilla(config-rtr)#exit

Barranquilla(config)#int f0/0

Barranquilla(config-if)#ipv6 rip simulacion enable

Barranquilla(config-if)#exit

Barranquilla(config)#int f1/0

Barranquilla(config-if)#ipv6 rip simulacion enable

Barranquilla(config-if)#exit

Barranquilla(config)#int f1/1

Barranquilla(config-if)#ipv6 rip simulacion enable

Barranquilla(config-if)#exit

Barranquilla(config)#exit

CONFIGURACION RIP BOGOTA

Bogota>enable

Bogota#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Bogota(config)#ipv6 unicast-routing

Bogota(config)#ipv6 router rip simulacion

Bogota(config-rtr)#exit

Bogota(config)#int f0/0

Bogota(config-if)#ipv6 rip simulacion enable

Bogota(config-if)#exit

Bogota(config)#int f0/1

Bogota(config-if)#ipv6 rip simulacion enable

Bogota(config-if)#exit

Bogota(config)#int f1/0

Bogota(config-if)#ipv6 rip simulacion enable

Bogota(config-if)#exit

Bogota(config)#exit

8.1.7 Implementación del protocolo DHCPv6. Protocolo DHCP (Protocolo de Configuración dinámica de host), es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

Cómo implementar DHCP para IPv6

Estos pasos nos mostraran los requerimientos básicos para implementar del DHCPv6.

1. Configuración de la función del servidor DHCPv6.
2. Configuración de un agente de base de datos de enlace para la función de servidor.
3. Configuración de la función de cliente DHCPv6.
4. Configurar el Agente de retransmisión DHCPv6.

➢ **Configuración de la función del servidor DHCPv6.**

Configuración de la piscina de configuración DHCPv6, esta tarea se realiza para crear y configurar el grupo de configuración de DHCPv6 y asociarlo a la piscina con un servidor en una interfaz.

Router> enable
Router # configure terminal
Router (config) # ipv6 dhcp pool pool1
Router (config-dhcp) # nombre de dominio example.com "Nombre del Dominio para una Cliente DHCPv6"
Router (config-dhcp) # dns-servidor 2001: DB8: 3000:3000 :: 42 "Especifica los Servidores DNS IPv6 disponibles a un cliente DHCPv6"
Router (config-dhcp) # prefijo delegación 2001: DB8: 1263 :: / 48 0005000400F1A4D070D03
Router (config-dhcp) # pool prefijo delegación pool1 vida 1800 60

Router (config-dhcp) # exit “salir del modo de configuración del modo de configuración del grupo de DHCPv6”
Router (config) # interface serial 3 “se especifica un tipo de interfaz”
Router (config-if) # ipv6 dhcp server pool1 “Activar DHCPv6 en una Interfaz”

- **Configuración de un agente de base de datos de enlace para la función de servidor.**

Router> enable
Router # configure terminal
Router (config) # ipv6 dhcp base de datos tftp :/ / 10.0.0.1/dhcp-binding

Este último especifica los parámetros del agente de Base de Datos del enlace.

- **Configuración de la función de cliente DHCPv6.**

Los Prefijos generales pueden definirse dinámicamente a partir de un prefijo recibido por un cliente que delega un prefijo DHCPv6. En conclusión esta tarea se realiza para configurar la función de cliente DHCPv6 en una interfaz y habilitar la delegación prefijo.

Router> enable
Router # configure terminal
Router (config) # int f0/0 “Especifica un tipo de interfaz y el número, y coloca el router en el modo de configuración de interfaz.”
Router (config-if) # ipv6 dhcp cliente pd dhcp-prefix “este comando activa el proceso de cliente DHCPv6 y permite una solicitud de delgacion de prefijo atraves de una interfaz específica”.

- **Configurar el Agente de retransmisión DHCPv6.**

Aquí se habilitan las funciones de agente de retransmisión DHCPv6 y especifique las direcciones de destino de retransmisión en una interfaz.

Router> enable
Router # configure terminal
Router (config) # int f4/2 “Especifica un tipo de interfaz y el número, y coloca el router en el modo de configuración de interfaz.”
Router (config-if) # ipv6 destino de retransmisión DHCP FE80 :: 250: A2FF: FEBF: A056 ethernet 4/3 “Especifica una dirección de destino a la que se envían los paquetes cliente y permite el servicio de retransmisión DHCPv6 en al interfaz”.

8.1.8 Comprobar compatibilidad de aplicaciones Ipv6. Después de configurar con direccionamiento IPv6 toda la red, encontramos los servidores que son host pero con capacidades mayores de administración, en estos encontramos instalados diferentes tipos de sistemas operativos, sobre los cuales corren diferentes aplicaciones, sin embargo en la implementación de IPv6 existen servicios cruciales como NIS, LDAP, DNS los cuales es importante verificar que las tablas estén actualizadas con las nuevas direcciones.

En dado caso que exista alguna aplicación que no sea compatible con IPv6 se debe analizar la forma de implementar una nueva aplicación que reemplace la existente pero que no paralice el funcionamiento de la empresa.

8.1.9 Implementación de medidas de seguridad para IPv6. La seguridad en IPv6 es un factor importante ya que al ser un protocolo de direcciones donde todas son públicas, lo que incurre en que el nivel de vulnerabilidad sea mayor, se tiene que estimar los recursos necesarios para la implementación de medidas de seguridad que garanticen la integridad de la información y la red.

Es recomendable activar todas las funciones de filtros, la utilización de la arquitectura de seguridad ip y demás funciones de seguridad necesarias para blindar a la empresa de cualquier ataque malicioso.

9. CONCLUSIONES

Con el desarrollo de este documento encontramos que es viable la migración entre ipv4 y ipv6, y sobre todo es necesario debido a que hoy por hoy la cantidad de direcciones ipv4 se han agotado, igualmente se pude concluir que las organizaciones pueden adoptar esta tecnología sin tener que cambiar todos sus dispositivos fiscos, no obstante deben realizar inversiones económica en dispositivos que sean compatibles con este protocolo los cuales devolverán la la inversión en funcionalidad y rendimiento.

IPv6 provee una funcionalidad similar a la ipv4, pero muchos de los mecanismos utilizados son diferentes, por tal motivo requiere de un análisis y planificación cuidadoso, las implicaciones de seguridad de ipv6 deben ser consideradas previo a su despliegue para evitar un impacto negativo, por ello es necesario que los administradores de los centros de cómputo en general cuenten con un soporte de ipv6 que les defina claramente las implicaciones de seguridad, por lo que es hora de capacitarse, entrenarse y experimentar.

Encontramos en IPv6 un gran cambio que dará solución al avance tecnológico, ya que en un futuro cercano todos los dispositivos electrónicos requerirán una dirección IP con la cual nos conectares desde cualquier lugar; descongestionando el funcional pero agotado IPv4.

Encontramos que IPv6 ofrece mejoras en sus funcionalidades, garantizando un mejor comportamiento en aspectos de configuración y seguridad.

Debido al agotamiento de las direcciones IPv4, es de suma importancia que todas las redes sean migradas lo antes posible al nuevo protocolo IPv6, para aprovechar todavía este tiempo que queda como tiempo de transición o tiempo de

experimentación para solventar los posibles inconvenientes que puedan darse en la migración.

En Colombia nos encontramos con un caso particular, ya que nuestros proveedores de internet no han avanzado hacia la implementación de IPv6 para suministrar a sus clientes. El cual se implica una limitante para que sus clientes migren exitosamente en su totalidad a la nueva versión de este protocolo.

BIBLIOGRAFIA

“Análisis Comparativo de los protocolos IPv6 e IPv4” [en línea], http://wb.ucc.edu.co/revistaingenieriasolidaria/files/2013/03/articulo-05-vol-5-n-9.pdf

“Coexistencia y Transsicion” [en línea], http://www.ipv6.cl/curso/SWF/ipv6_mod9.htm

“Como Conectar Subredes a la Red” [en línea], http://www.ehowenespanol.com/conectar-subredes-red-como_218665/

“Como son las Direcciones IPv6” [en línea], http://www.uroboros.es/como-son-las-direcciones-ipv6/

“Diferencia entre IPv4 e IPv6” [en línea], http://kb.linksys.com/Linksys/GetArticle.aspx?docid=5ffa2d2066e04baebbd86f1da1a4c0a8_Diferencias_entre_IPv4_e_IPv6.xml&pid=82&converted=0

“Dirección IPv6” [en línea], http://alemodeloosi.blogspot.com/2010/11/direccion-ipv6.html

“Dirección IPv6” [en línea], http://msdn.microsoft.com/es-es/library/95c9d312(v=vs.80).aspx

“El Modelo OSI” [en línea], http://www.oocities.org/dralkzta/osi.htm

“Modelos de Protocolos y Referencia” [en línea], http://crstn45.blogspot.com/p/modelos-osi-y-tcpip.html

“Modelos OSI y TCP/IP” [en línea], http://modelos-osi-y-tcp-ip-anica.blogspot.com/

“Protocolos de Descubrimiento de Vecino” [en línea], http://redes-ipv6.blogspot.com/2008/11/protocolo-de-descubrimiento-de-vecino_14.html

“Saga IPv6 Episode II: Direcciones IPv6 Formato y Tipos” [en línea], http://lobobinario.blogspot.com/2011/03/saga-ipv6-episode-ii-direcciones-ipv6.html

“Saga IPv6 Episode III: Plan de Direccionamiento en IPv6” [en línea], http://lobobinario.blogspot.com/2011/03/saga-ipv6-episode-iii-plan-de.html

“Seis Pasos para Migrar de IPv4 a IPv6” [en línea], http://www.techweek.es/infraestructuras-tic/informes/1008310003701/seis-pasosmigrar-ipv6.1.html

“Tipos de Direcciones IPv6: Unicast, AnyCast, Multicast” [en línea], http://ipv4to6.blogspot.com/p/tipos-de-direcciones-ipv6-unicast.html

AHUZTZIN, Gerardo. “Desarrollo de un esquema de traducción de Direcciones IPv6-IPv4-IPv6” [en línea],

APARICIO, Rubén. “La migración segura de IPv4 a IPv6: los tres pasos básicos” [en línea], http://www.networkworld.es/actualidad/la-migracion-segura-de-ipv4-a-ipv6-los-tres-pasos-basicos

Autores Varios, “Comparación entre IPv4 – IPv6” [en línea], http://www.ilustrados.com/documentos/eb-Comparacion%20IP4%20y%20IPV6.pdf

ÁVILA MEJÍA, Oscar. “Migración del protocolo IPv4 a IPv6” [en línea] http://www.izt.uam.mx/newpage/contactos/anterior/n79ne/ipv6.pdf

Gobierno, de España “IPv6 Protocolo de Internet Versión 6” [en línea], http://www.ipv6.es/es-ES/transicion/quees/Paginas/Transicion.aspx
http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Institución, Universitaria ITM “Configuración e Implementación de Redes de Datos con Direccionamiento IPv4 e IPv6” [en línea], http://es.scribd.com/doc/44342778/Tdg-Ipv4-Ipv6-18n0v

IPv6, MX “Fundamentos de IPv6” [en línea], http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Tesis en línea http://biblioteca.ucp.edu.co:8080/jspui/bitstream/10785/958/1/completo.pdf

Traducciones, howtos – Unix – Linux –Windows y redes [en línea], http://www.tecnodelinglesalcastellano.com/2011/04/protocolo-de-internet-version-4-ipipv4.html

Universidad, de la Republica Uruguay “Introducción al IPv6” [en línea], http://www.rau.edu.uy/ipv6/queesipv6.htm

Universidad, Técnica del Norte “Análisis del Protocolo IPv6 su Evolución y Aplicabilidad” [en línea], http://repositorio.utn.edu.ec/bitstream/123456789/619/1/CAPITULO1.pdf

Universidad, Técnica Federio Santa María “IPv4 – IPv6” [en línea], http://profesores.elo.utfsm.cl/~agv/elo322/1s10/project/reports/Informe%20IPv4IPv6%20%20%20%20Yair%20Dur%C3%A1n%202921065-9%20%20%20%20%20Daniel%20Veas%20176884649.pdf