

Implementación del protocolo IPv6 en la compañía J Walter Thompson Colombia

Presentado por:

Giovanny Cárdenas Rodríguez

Fundación Universitaria los Libertadores

Facultad de Ingeniería y Ciencias Básicas

Ingeniería de Sistemas

Bogotá D.C

2018

Implementación del protocolo IPv6 en la compañía J Walter Thompson Colombia

Presentado por:

Giovanny Cárdenas Rodríguez

Proyecto de Grado para Optar el Título de Ingeniero de sistemas

Ingeniero Augusto José Ángel Moreno
Director

Fundación Universitaria los Libertadores
Facultad de Ingeniería y Ciencias Básicas
Ingeniería de Sistemas

Bogotá D.C

2018

Tabla de contenido

RESUMEN	1
PALABRAS CLAVES:	1
ABSTRACT	2
Glosario	3
1. Introducción	5
2. Planteamiento del problema	6
3. Justificación	7
4. Alcance y Limitaciones	8
5. OBJETIVOS	9
5.1 General	9
5.2. Específicos	9
6. MARCO TEORICO	10
6.1 Internet	10
6.2 Componentes en una Red	10
6.3 Modelo Referencia OSI	11
6.4 Protocolos TCP/IP	12
6.5 Medios de transmisión en la red	13
6.6 Definición Internet Protocol (IP)	15
6.7 Definición de IPv4	14
6.8 Características de IPv4	15
6.9 Tipos de Direcciones	15
6.10 Tipos de comunicación	16
6.11 Definición y Clases de Direcciones	16
6.12 Definición direcciones privadas y públicas	17
6.13 Necesidad de Utilizar IPv6	18
6.14 Características del protocolo IPv6	19
6.15 Transición IPv6	19
6.16 Representación de una dirección IPv6	19
6.17 Reglas para reducir una Dirección IPv6	20
6.18 Longitud de prefijo IPv6	22
6.19 Direcciones IPv6 de Unifusión	22
6.20 Estructura de una dirección IPv6	23
6.21 Direcciones IPv6 Link Local Dinámicas	24
6.22 Direcciones IPv6 link Local estáticas	25
6.23 Protocolos de enrutamiento IPv6	25
6.24 Tipos de Direcciones IPv6	25
6.25 Tecnología de Transición (Dual Stack)	25
6.26 Tipos de túneles empleados como tecnologías de transición	27

7. INGENIERIA DEL PROYECTO	29
7.1 Descripción actual	29
7.2 Requerimientos de la Información	29
7.2.1 Hardware y Software	29
7.2.2 DNS y DHCP	30
7.2.3 Servicios y Aplicaciones	30
7.2.4 Inventario IT	30
7.3 Modelamiento del sistemas	34
7.4 Descripción del sistema	35
8. EVALUCIACIÓN ECONÓMICA DEL PROYECTO	36
8.1 Riesgo en fase de analisis	36
8.2 Riesgo en fase de diseño	36
8.3 Riesgo en fase de codificación	37
8.4 Riesgo en fase de prueba	37
8.5 Riesgo en fase de implementación	38
8.6 Riesgo en fase de mantenimiento	38
9. PRESUPUESTO DETALLADO	39
9.1 Costo de infraestructura fisica	39
9.2 Costo total del proyecto	39
10. BENEFICIOS DE LA IMPLEMENTACIÓN	40
10.1 Operacionales	40
10.2 De gestión	40
10.3 Estratégicos	40
10.4 De infraestructura	40
10.5 De IT	41
11. CRONOGRAMA	42
12. RECOMENDACIONES	43
13. CONCLUSIONES	44
BIBLIOGRAFIA	45

Lista de Tablas

Tabla 1: Inventario de Switches & Router ----- 32

Tabla 2: Inventario De APS ----- 32

Tabla 3: Inventario Servidores ----- 33

Tabla 4: Costo1 ----- 39

Tabla 5: Costo 2 ----- 39

Tabla 6: Costo 3 ----- 39

Lista de Figuras

Figura 1:	Red de Internet-----	10
Figura 2:	Componentes de una red -----	11
Figura 3:	Protocolos TCP/IP-----	12
Figura 4:	Tipos de Direcciones -----	16
Figura 5:	Clases de Direcciones -----	17
Figura 6:	Agoatamiento IPv4 -----	18
Figura 7:	Representación de una dirección IPv6 -----	19
Figura 8:	Regla 1 -----	20
Figura 9:	Ejemplo 1 Regla 1 -----	20
Figura 10:	Ejemplo 2 Regla 1 -----	20
Figura 11:	Ejemplo 3 Regla 1 -----	20
Figura 12:	Regla 2 -----	21
Figura 13:	Ejemplo 1 de Regla 2-----	21
Figura 14:	Ejemplo 2 de Regla 2-----	21
Figura 15:	Ejemplo 3 de Regla 2-----	21
Figura 16:	Longitud de prefijo IPv6-----	22
Figura 17:	Dirección Global -----	23
Figura 18:	Dirección Link Local -----	24
Figura 19:	Dual Stack-----	26
Figura 20:	Tunelización-----	27
Figura 21:	Traducción NAT64 -----	28
Figura 22:	Diagrama de red -----	31
Figura 23:	Modelamiento nueva configuración-----	34
Figura 24:	Cronograma-----	42

Resumen

En febrero del 2011 Nos informa IANA (Internet Assigned Numbers Authority) administrador del stock central de las direcciones IPv4. Que quedaron disponibles 5 bloques de mascara /8, los cuales se entregaron a los RIPS correspondientes. A partir de ese momento cada RIPS empezaron a disponer de los últimos bloques que contaban y esto produce ya un agotamiento de direcciones ipv4. En estos momentos a nivel mundial se encuentran zonas con registros regionales sin recursos. Desde ya tenemos que pensar en una internet basada en ipv6. Se espera que las grandes compañías y pequeñas estén adoptando al nuevo protocolo IPV6.

De acuerdo con lo anterior, el protocolo IPv4 que se utiliza actualmente. No puede cubrir el crecimiento de direccionamiento por tanto desarrollo y crecimiento de las redes que actualmente existen. Lo que se quiere con IPv6 es aliviar toda la demanda del direccionamiento en todo el mundo, para nuevas aplicaciones y dispositivos. La solución es migrar todo el protocolo IPv4 a IPv6. Es decir, ir abandonando poco a poco la versión 4 e ir implementando la nueva versión. Para hacer este paso no tan brusco tenemos unos mecanismos de transición que nos ayudará a que este paso sea lo suficiente seguro, y tengamos la mejor experiencia en esta migración.

Los mecanismos de migración como son Dual Stack, Tunnelización y traducción. Nos ayudan a realizar este paso de transición en una manera más sencilla a todas las compañías. Y de esa forma hacer todos los pasos necesarios para lograr una correcta migración donde obtendremos muchos beneficios.

Palabras Claves: IPV4, IPV6, Protocolo de Internet, ICMP6, Protocolos de Enrutamiento, DHCP, Dual Stack

Abstract

In February 2011, the administrator of the central stock of the IPv4 addresses -IANA (Internet Assigned Numbers Authority)- reported that only were available 5 mask blocks /8, and its were delivered to the corresponding RIPS. From that moment on, each RIPS began to have the last blocks they had, generating an lacking of IPv4 addresses. At present time, worldwide, there are areas with regional registers without resources. Then people need already have to think about an IPv6-based internet. It is expected that large and small companies are adopting the new IPV6 protocol.

Due to the above, the IPv4 protocol that is currently used cannot cover the growth of addressing because of the development and growth of the networks that currently exist. The IPv6 pretends to improve all the demand for addressing around the world, for new applications and devices. The solution is to migrate from IPv4 protocol to IPv6. That is, gradually abandon version IPv4 and implement the new version. For this change to be transparent, there are some transition mechanisms that will help to have safe and reliable migration.

These migration mechanisms are Dual Stack, Tunneling and translation and will help go to the transition in a simpler way for all companies. Executing all the necessary steps to achieve a correct migration and with much benefits

Key Words

IPv4, IPv6, Internet Protocol, ICMPv6, Routing Protocols, DHCP, Dual Stack

Glosario

Binario

Sistema utilizado para pasar de decimal a binarios el protocolo ipv4 y realizar subnetting.

Broadcast

Paquete de datos enviado a todos los hosts de la compañía generando actualización o enviando un ataque a toda la red.

Colisión

En Ethernet, se produce cuando dos nodos intentan realizar la comunicación simultáneamente.

Enrutamiento

El Protocolo de enrutamiento, es utilizado para determinar la mejor ruta del origen al destino, de acuerdo con el costo y la métrica. Tenemos RIP, EIGRP, Y OSPF internamente.

Gateway

Es una interfaz configurada en un equipo de capa 3 para brindarle servicios a los hosts.

Host

Hace referencia a una computadora ya sea un portátil o equipo de escritorio. Que pertenece a una red.

HUB

Dispositivo conocido como repetidor utilizado en una topología en estrella. Pero genera muchas colisiones y por eso es mucho mejor utilizar un Switch.

Internet

Es un conjunto de redes donde se conectan routers y otros dispositivos que conforman esa gran red.

IP

Protocolo de internet, de la capa del modelo OSI de capa de red de la pila TCP/IP que ofrece el servicio de internetwork no orientado a la conexión.

Ipssec

Es un conjunto de medidas orientado a la seguridad para proteger las transmisiones del protocolo IP.

Ipv6

Abreviatura escogida por la IETF para identificar al nuevo protocolo IP.

Ping

Comando que se utiliza y el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de red. Para probar el alcance de un dispositivo.

Router

Dispositivo de capa de red que utiliza sus interfaces ya sean lan o wan y una tabla enrutamiento para enviar el paquete a la mejor ruta.

Tunnelling

Encapsulado de un protocolo IPV6 dentro del protocolo Ipv4 o viceversa.

1. Introducción

Internet es una internetwork, es la red más grande donde encontramos conectividad en todas las ciudades y países de todo el mundo. En ella encontramos servicios de voz sobre IP, mensajería instantánea, streaming y cantidad de servicios. que nos hace la vida más fácil en nuestra comunicación. En la actualidad ipv4 se diseñó para tener en cada empresa y hogar su dirección pública como privada. Esto nos lleva a cada compañía a tener su dirección IP pública y un segmento de red privado, ya sea clase A, B o C dependiendo la cantidad de usuarios que tiene la compañía, y cada host se le asignará su IP privada.

Por eso se pensó en ipv4 de 32 bits, cuando se estandarizó y se convirtió en una arquitectura de cobertura mundial. Donde internet fue fundada con fines de investigación científicos, técnicos, y objetivos militares. Hoy al hablar de internet que es la columna principal de las comunicaciones y la herramienta imprescindible en una compañía y hogar. Por tanta demanda no tuvo más recursos para seguir adelante y llega la nueva versión que es ipv6 de 128 bits.

Es necesario recuperar la conectividad extremo a extremo. El agotamiento de direcciones IPv4 no es algo nuevo y en los últimos años, una de las medidas adoptadas ha sido el uso de traductores de direcciones (NAT). Estos traductores de direcciones implican que no es posible la conexión directa extremo a extremo y como consecuencia, solo funcionan correctamente las aplicaciones cliente-servidor, y por tanto Internet se ha convertido en una red mucho más compleja, cara y difícil de gestionar. IPv6 tiene tantas direcciones que no necesitamos utilizar NAT para publicar un servidor al exterior para conectarse remotamente o cámaras de la compañía para conocer en tiempo real lo que está pasando.

La idea es implementar un mecanismo de transición de ipv4 a ipv6 para la compañía donde no se vean afectados sus servicios y operaciones de sus procesos diarios. Pero es una migración que se debe realizar paso a paso conociendo muy bien su infraestructura empezar realizar muy bien la implementación.

2. Planteamiento del problema

En el comunicado de la IANA (Internet Assigned Numbers Authority) nos informa que el protocolo de internet versión 4 se está agotando desde el año 2011. Para brindarle una mejor solución a nivel mundial. Se creó un nuevo protocolo IPv6 con mejores características. Para que todas las compañías puedan realizar la transición al nuevo protocolo con el propósito de brindarles una mejor conectividad y servicios.

Es un asunto muy importante para todas las compañías en llevar su infraestructura de comunicaciones a IPv6. Se tiene que realizar un riguroso levantamiento de información de todos sus equipos de comunicación con el fin de saber si cumplen con lo necesario para soportar IPv6 o deben adquirir nuevos equipos. No todas las compañías cuentan con una infraestructura óptima para realizar dicha transición y seguir con los pasos necesarios para que sea un proceso transparente para toda la compañía. Saben que para este proceso se necesita un presupuesto económico y personas expertas que trabajen de la mano con el área IT.

Con la información anterior, la compañía J Walter Thompson no tiene un conocimiento claro de toda su infraestructura. Se requiere realizar un levantamiento de información de todos sus equipos de comunicaciones y topología de red actual a nivel físico y lógico. La información se debe clasificar en las siguientes categorías:

A nivel de hardware encontramos: Switches, Routers, Servidores, APS, y PCS,
A nivel de Software encontramos: Aplicaciones de Nomina, IOS de Switches, Routers y APS, Sistema operativo de servidores y otras aplicaciones.

Con el fin de empezar a analizar y plantear su transición cuanto antes y más adelante no los tomen desprevenidos en una transición más obliga y con menos tiempo. Se deben seguir los pasos planteados por un experto para tomar la decisión del mecanismo que se va a utilizar de acuerdo a la información recopilada y demás investigaciones necesarias de la infraestructura para ejecutar un buen plan de trabajo.

3. Justificación

El proyecto de J Walter Thompson surge con la necesidad de realizar su transición de toda su infraestructura del Protocolo IPv4 al nuevo protocolo de Internet que es IPv6. Esta migración es un proceso que se debe ir optando no solo en J Walter Thompson, si no para compañías privadas como públicas. El propósito de este proyecto es actualizar su protocolo de internet que utilizan actualmente sin afectar sus aplicaciones internas y procesos que en la actualidad la compañía realiza. La idea es obtener muchas características y beneficios del nuevo protocolo con el fin de mejorar la seguridad a nivel de capa 3, y conectar muchos equipos. Esa era una desventaja en el protocolo IPv4 que en el nuevo ya no existe.

Con lo anterior y conociendo la necesidad de la compañía se identifica que no tienen conocimiento de este proceso y conocimiento de esta transición. Este paso lo debe manejar un experto para establecer un plan de trabajo de toda la infraestructura y plantear el mecanismo de transición adecuado claramente conociendo la operación de la empresa para que no se vea afectada en este cambio, Para que sea un proceso muy transparente.

Actualmente todas las compañías de desarrollo de hardware como de software ya están estableciendo IPv6 en sus productos. Es necesario dar este paso con el fin de aprovechar muchas ventajas que pueden favorecer a la compañía. Como sabemos IPv6 fue pensado para el futuro de nuevos edificios inteligentes, casas inteligentes, nuevas innovaciones a nivel de sensores y nivel de hardware para motivar en el desarrollo y no tener limitantes.

IPv6 fue desarrollado para cubrir las necesidades de grandes compañías y pequeñas. Se veían afectadas por el límite que tenían con IPv4. Pero habilitando el nuevo protocolo se espera que se tenga un crecimiento a nivel como se mencionó anteriormente en nuevos desarrollos en aplicaciones y a nivel de hardware.

De acuerdo con toda la información anteriormente, se desea en J Walter Thompson diseñar una red donde la pila de protocolos IPv4 e IPv6 trabajen simultáneamente y ofrecer beneficios que le ofrece el nuevo protocolo. Adicionalmente pensar en cómo aprovechar los beneficios.

4 Alcance y Limitaciones Del Proyecto.

4.1 Alcance

La Migración de la Topología Lógica tiene como objetivo principal en configurar Dual Stack donde los dos protocolos IPv4 e IPv6 convivan en la misma red. permitiendo que los hosts, servidores, aplicaciones y equipos de comunicaciones se puedan comunicar interno como externo utilizando alguno de los dos protocolos.

4.2 Limitaciones

- Información incompleta del inventario.
- Poco conocimiento de la infraestructura por parte del área IT.
- Falta de conocimiento del nuevo protocolo y sus mecanismos de transición.
- Solicitar permisos a terceros para ver configuración de los equipos de comunicaciones de la compañía.
- Poco presupuesto económico por parte de la compañía.

5 Objetivos

5.1 General

Diseñar e implementar el mecanismo de transición Dual Stack en la red actual, para el funcionamiento de IPv4 e IPv6 garantizando la comunicación interna y externa de ambos protocolos

5.2 Específicos

- Brindar una migración confiable y segura.
- Reducir costos favoreciendo a la compañía.
- Desarrollar una documentación para capacitar al área IT de dicha transición.
- Definir el plan de trabajo para lograr la transición.
- Interpretar las necesidades del cliente.
- Determinar un mecanismo de transición para la migración al nuevo protocolo.

6. Marco Teórico

6.1 Internet

Internet es una colección global de redes interconectadas (Internet Works o internet para abreviar). Internet se puede observar como una recopilación entre LAN y WAN.

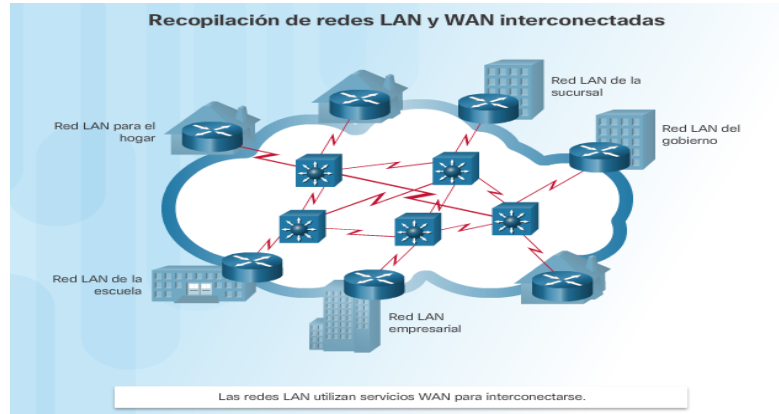


Figura 1: Red Internet

Para garantizar una buena comunicación efectiva en esta infraestructura heterogénea que requiere la aplicación de estándares y tecnologías uniformes que utilizan la familia TCP/IP para garantizar su comunicación. Existen organizaciones que se desarrollaron con el fin de ayudar a mantener la infraestructura y los estándares de los protocolos y los procesos de internet. Sus orígenes se remontan a 1969.

6.2 Componentes de una red

Esta infraestructura de la red proporciona el canal estable y confiable por el cual se producen las comunicaciones.

La infraestructura de red contiene tres categorías de componentes de red.

- Dispositivos
- Medios
- Servicios

Los dispositivos y los medios son los elementos físicos o hardware de la red. Y los servicios incluyen una gran cantidad de aplicaciones de red comunes que incluyen las personas a diario como es el correo y las aplicaciones web.

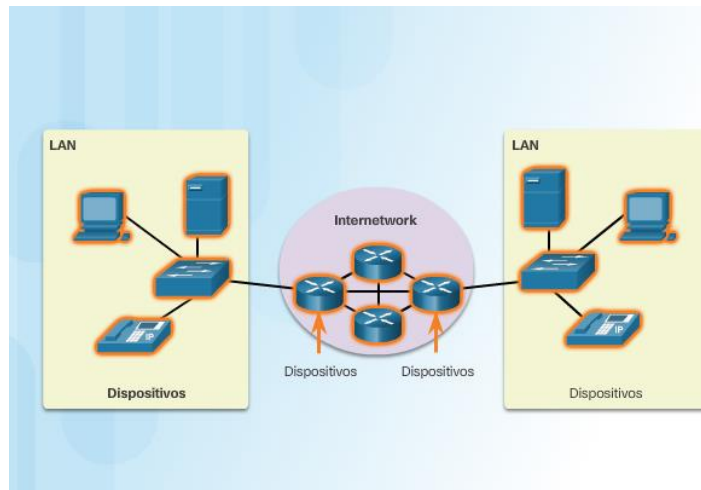


Figura 2: Componentes de una Red

6.3 Modelo de referencia OSI.

El modelo OSI representa funciones y servicios en cada capa. Donde cada una describe la interacción de abajo hacia arriba y viceversa. El modelo OSI fue propuesto por ("Organización Internacional de Estándares") por esa razón dividen la comunicación en capas para entender mucho mejor la comunicación.

Las capas del modelo OSI se mencionan más con frecuencia por el número y no por el nombre.

- **Aplicación:** La capa de aplicación contiene protocolos utilizados para comunicaciones de procesos.
- **Presentación:** La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
- **Sesión:** La capa de sesión proporciona servicios a la capa de presentación para organizar su dialogo y administrar el intercambio de datos.
- **Transporte:** Define los servicios de segmentación, reensamblar y transferir los datos para las comunicaciones individuales entre terminales.
- **Red:** La capa de red brinda el servicio de intercambiar los datos con el protocolo enrutamientos en redes locales como remotas.

- **Enlace de datos:** Este protocolo describe los métodos de intercambiar tramas de datos entre los dispositivos en un medio común.
- **Físico:** La capa física describe los medios mecánicos por donde viajan los bits transmitidos. Mantener y desactivar los medios.

6.4 Protocolos TCP/IP

Es conocido como el modelo de internet se define en 4 categorías donde aplican las funciones que deben seguir para establecer una comunicación correctamente. El modelo TCP/IP es un estándar abierto.

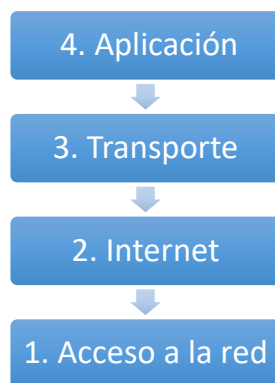


Figura 3: Protocolos TCP/IP

La primera capa es de acceso a la red, es la encargada del intercambio de datos entre un host a una red remota por un medio. Define todos los procedimientos necesarios para que un host tenga acceso a la red.

La segunda capa es la de Internet es igual a la capa de red del modelo OSI. Su propósito es escoger la mejor ruta “camino” para un paquete a través de todas las redes. Desde la estación de origen hasta el destino.

La tercera capa de transporte es la responsable de transmitir los paquetes del origen hacia el destino, lleva un control de cada segmento transmitido dependiendo de que protocolo se utilice, puede corregir los errores y retransmitir los segmentos que no llegaron o llegaron incompletos a su destino. El protocolo responsable para realizar dicha tarea es TCP. Es confiable y orientado a la conexión.

El siguiente **Protocolo es UDP**, no es orientado a la conexión, y es más utilizado en video juegos donde no se necesita una transmisión segura.

La cuarta capa de aplicación, En este nivel encontramos que es la más cercana al usuario final. Es la encargada de proporcionar la interfaz entre las aplicaciones utilizadas para la comunicación en la cual se transmiten los mensajes. Depende de los protocolos de la capa de aplicación que se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Programas y su correspondiente protocolo: http("Hypertext Transfer protocol"), FTP("File Transfer Protocol"), SMTP("Simple Mail Transfer Protocol"), DNS("Domain Name System") entre otros.

6.5 Medios de transmisión en la red.

- **Cableado de cobre**

Se utilizan en redes por su economía y fáciles de instalar y tienen baja resistencia a la corriente eléctrica, pero se ven limitados por dos razones por la distancia y la interferencia en las señales. Los datos se transmiten como impulsos eléctricos.

Existen tres tipos de medios de cobre que se utilizan en las redes.

Par trenzado no blindado (UTP)

Par trenzado Blindado (STP)

Coaxial

Estos cables se utilizan para interconectar los nodos en una LAN y los dispositivos de infraestructura. Como son los Switches, Routers, Firewall y puntos de acceso inalámbrico. Utilizan un único conector físico para diferentes tipos de conexiones. Por ejemplo, el conector Rj-45 se utiliza para las redes LAN, y para redes WAN utilizan otro medio de transmisión.

- **Cable Par Trenzado no Blindado**

Este tipo de cable es par trenzado no blindado. Es el medio de red más común utilizado. Consta de 4 pares de hilos codificados por colores que se encuentran trenzados entre si y recubiertos con un revestimiento de plástico flexible que los protege contra daños físicos menores. La principal ventaja en tener los hilos trenzados es que nos ayuda a proteger contra las interferencias señales de otros hilos.

- El cableado UTP cumple con los estándares establecidos por la TIA/EIA-568

- Existen diferentes cables que son: Cable directo Ethernet, Cable Cruzado Ethernet y cable de consola. De acuerdo con la norma establecida en el cable.

- **Cable de par trenzado Blindado.**

Este tipo de cable (STP) nos brinda una mejor protección contra el ruido que el cable UTP. En comparación con UTP es más costoso y difícil de instalar. La técnica de blindaje es para contrarrestar la EMI, la RFI y lo trenzado es para reducir el crosstalk.

- **Cable Coaxial**

Este tipo de cable contiene dos conductores que comparten el mismo eje. Tiene el conductor es por donde se transmite las señales electrónicas. Cuenta con una capa de aislamiento plástico flexible que rodea el conductor de cobre.

La totalidad del cable está cubierta por un revestimiento para evitar daños físicos.

- **Fibra óptica**

Se compone de dos tipos de vidrio (Núcleo y revestecimiento) y un blindaje exterior de protección. La fibra es muy delgada y envía pulsos de luz que representan los datos transmitidos en forma de Bits.

Los cables de fibra óptica se pueden clasificar en:

Fibra óptica Monomodo (SMF) envía un único haz de luz.

Fibra óptica multimodo (MMF) la luz de un LED ingresa a la fibra multimodo en diferentes ángulos.

6.6 Definición Internet Protocol (IP)

Es la base fundamental de internet para la transferencia de paquetes. Es el encargado de tomar el mejor camino para llegar a su destino. IP ofrece un servicio de mínimo esfuerzo, es decir: entrega los paquetes, pero no es responsable si se pierden en el transcurso del camino, o se corrompen y se desordenan. En lo dicho anteriormente IP no ofrece un servicio seguro. Se crea el protocolo de control de transmisión que es TCP, fue desarrollado para dar seguridad a la transferencia de cadenas de información usando el protocolo orientado no a la conexión IP. TCP ofrece un servicio que funciona de extremo a extremo para el control de flujo y de

errores que surgen de perder, retardar o entregar equivocadamente los paquetes IP. Cuando el tráfico de una red se congestiona los paquetes se empiezan a descartar. La recuperación de los paquetes perdidos es responsabilidad de los extremos de la red. Las direcciones IP consiste en cuatro octetos cada octeto representa 1 byte y separados por un punto. En total son 32 bits que se expresan en número decimal. Las direcciones IP consiste en dos partes una identificación de red y uno de host. Cada host utiliza una dirección única en una red local también conocidas como IP Privada. También están las direcciones públicas que las utilizan los proveedores ISP para dar conectividad hacia la internet y es única para cada entidad. En actualidad encontramos dos tipos de protocolos de internet. están IPV4 y IPV6 mas adelante hablaremos de cada protocolo IP.

6.7 Definición de IPV4

Es la versión 4 del Protocolo Internet ("internet Protocol"). Este fue el primer protocolo que fue lanzado en 1981. Se convierte en el principal protocolo utilizado en el modelo TCP/IP para internet. Es utilizado para la comunicación entre redes. Están divididas en clases privadas y públicas. A partir de 1992 se empezó a revisar mecanismos para una nueva versión por motivo que la tecnología iba creciendo en cuanto a aplicaciones y host y no daría la versión 4 a tener direcciones para soportar la demanda en las comunicaciones de redes. Pero si debemos saber que a partir el 31 de enero del 2011 las direcciones IPV4 quedaron agotadas y no es posible más su crecimiento por esa razón se creó la nueva versión de protocolo de internet llamado IPV6 nos trae nuevos beneficios más adelante hablaremos de este nuevo protocolo

6.8 Características IPV4

- Es un protocolo de envío de paquetes no confiable.
- No garantiza la entrega del paquete.
- No garantiza el orden ni la retransmisión del paquete por si se pierde

Todos esos problemas se resuelven con el modelo TCP/IP atreves de TCP o UDP.

6.9 Tipos de Direcciones

Dirección de Red: Es una manera estándar en referirse a una red. Por ejemplo 10.0.0.0/8, hace referencia a una red privada asignada a una compañía.

Dirección de Host: Cada dispositivo final requiere una dirección única para enviar un paquete a un destino. Se asigna su dirección IP, mascara subred y Gateway.

Dirección de Broadcast: Se establece una dirección especial para cada red. Que permite la comunicación a todos los hosts de dicha red. Un solo dispositivo final

puede enviar un paquete a todos los demás. La dirección de broadcast es la dirección más alta.

	Red			Host
Dirección de red	10	0	0	0
	00001010	00000000	00000000	00000000
Dirección de broadcast	10	0	0	255
	00001010	00000000	00000000	11111111
Dirección host	10	0	0	1
	00001010	00000000	00000000	00000001

Figura 4: Tipos de Direcciones

6.10 Tipos de comunicación

En una red IPV4 Existen 3 formas de comunicación entre hosts.

Unicast: En este proceso un host envía un paquete a un host individual.

Broadcast: Un host puede enviar un paquete a todos los hosts de la misma red.

Multicas: Un host puede enviar un paquete al seleccionar solo a un grupo de hosts.

6.11 Definición clases de direcciones de acuerdo a la RFC1700

Clase A: El diseño está definido para redes muy grandes, donde la compañía necesita conectar muchos hosts. Tiene aproximadamente 16 mil millones de IPS. Y utilizan mascara /8. Donde el primer octeto indica la dirección de red y los demás octetos están ceros para asignarlos a hosts.

Clase B: Fue diseñado para satisfacer empresas medianas de un tamaño no tan grande. Que puede cubrir un total de 65.000 mil hosts con una máscara de /16. Los dos primeros octetos indica la red, y los otros dos restantes son para direcciones IPS válidas para hosts.

Clase C: Este espacio de direcciones de clase C son las más antiguas y comúnmente disponibles. Con un propósito de proporcionar un máximo de direcciones validas 254. Utilizan el prefijo de mascara /24.

El bloque de Dirección clase C reserva un espacio para las redes de clase D, que se utiliza para multicast y clase E para experimental mediante el valor de uso fijo 110 para los 3 primeros bits más significativos.

Clase de dirección	Rango del primer octeto (decimal)	Bits del primer octeto (los bits verdes no se modifican)	Partes de las direcciones de red (N) y de host (H)	Máscara de subred predeterminada (decimal y binaria)	Cantidad de posibles redes y hosts por red
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16777214 hosts por red ($2^{24}-2$)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16384 redes (2^{14}) 65534 hosts por red ($2^{16}-2$)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2097150 redes ($2^{21}-2$) 254 hosts por red (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

Figura 5: Clases de Direcciones

6.12 Definición de Direcciones privadas & Públicas:

Las direcciones privadas son utilizadas en redes internas. establecido en la RFC 1918, estas direcciones no son enrutables por internet. Por lo general los hosts utilizan estas direcciones privadas. Se tiene que garantizar que cada host utilice una única dirección dentro su entorno de networking. En diferentes empresas pueden utilizar el mismo segmento. Estas direcciones privadas no tienen enrutamiento, se tiene que realizar un NAT para traducir esa dirección privada a una publica para salir a internet.

Estas son las direcciones privadas.

10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Las direcciones **públicas** son las que se enrutan globalmente entre los routers de los ISP ("Proveedores de servicio de internet").

6.13 Necesidad de utilizar IPV6

El principal motivo fue el agotamiento de direccionamiento en el protocolo IPv4. Fue el factor para comenzar a pensar y desarrollar un nuevo protocolo para corregir esta desventaja de limitaciones. IETF comenzó a desarrollar el nuevo protocolo IPv6 de 128 Bits incluyendo mejoras en sus características para satisfacer las demandas.

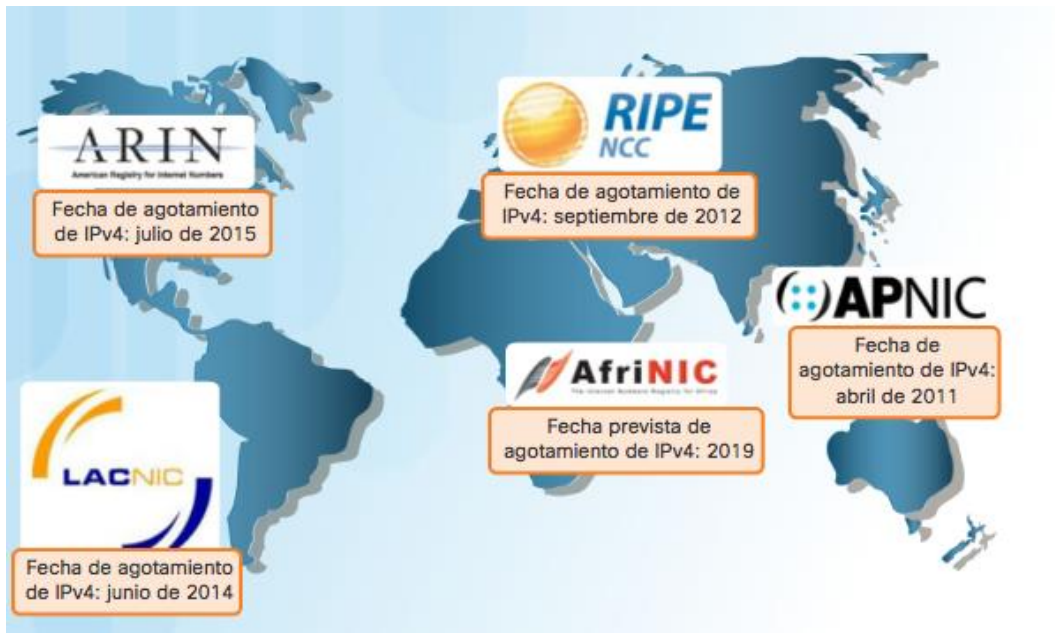


Figura 6: Agotamiento IPv4.

Como podemos observar en la figura 6. Nos indica el agotamiento de IPv4, fue el factor que motivó la migración a IPv6. Debido al aumento significativo de conexiones a internet como en Asia, África y en otras áreas del mundo. Las direcciones IPv4 ya no son suficientes como para admitir más crecimiento.

IPv4 tiene un máximo de 43000 millones de direcciones. Las direcciones privadas Utilizaron NAT. Sin embargo, NAT rompe muchas aplicaciones y tiene limitaciones. Con IPv6 ya no es necesario utilizar NAT.

6.14 Características del protocolo IPv6

- Direccionamiento jerárquico de 128 Bits. Para crecer el direccionamiento jerárquico.
- Simplificar el formato encabezado, con el fin de mejorar el manejo de paquetes.
- Soporte mejorado para extensiones y opciones para la mejor escalabilidad.
- Capacidades de autenticación y privacidad para integridad seguridad.

6.15 Transición IPv6

IPv6 ha sido diseñado con escalabilidad para permitir años de crecimiento de la Internet. El nuevo protocolo se está implementando lentamente. IPv4 se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro. Pero poco a poco IPv6 será el protocolo de internet dominante.

6.16 Representación de una dirección IPv6

Como lo mencionamos anteriormente tiene una longitud de 128 Bits, y se escribe como una cadena de valores hexadecimales. Un dígito decimal se identifica como 4 bits para llegar a ser un hexteto representa 16 bits. En total son 8 hextetos=128 Bits.

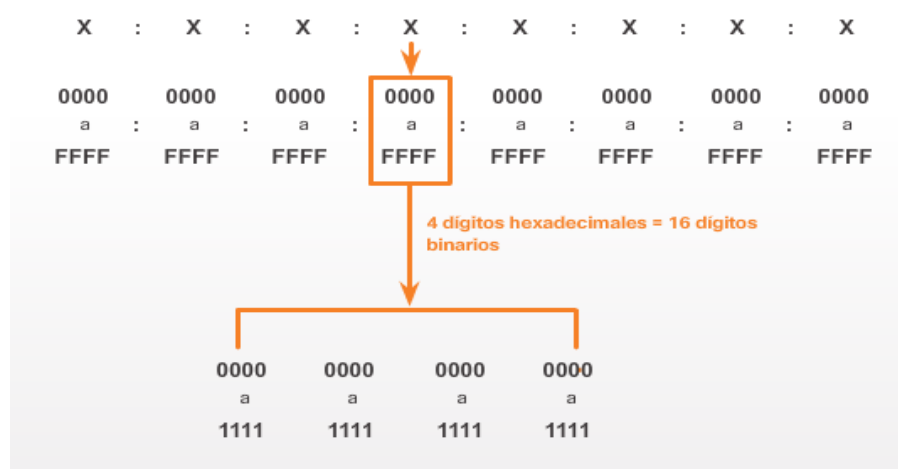


Figura 7: Representación de una dirección IPv6

6.17 Reglas para reducir una dirección IPv6

1. Omitir los ceros iniciales, es la primera regla para reducir una dirección ipv6 en cualquier sección de 16 bits o Hexteto. Esta regla solo aplica a ceros iniciales no para ceros finales de lo contrario se convertiría en una dirección ambigua.

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin ceros iniciales	2001: DB8: 0:1111: 0: 0: 0: 200

Figura 8: Regla 1

Ejemplos:

Recomendado	2001:0DB8:0000:A300:ABCD:0000:0000:1234
Sin ceros iniciales	2001: DB8: 0:A300:ABCD: 0: 0:1234

Figura 9: Ejemplo 1 Regla 1

Recomendado	2001:0DB8:000A:1000:0000:0000:0000:0100
Sin ceros iniciales	2001: DB8: A:1000: 0: 0: 0: 100

Figura 10: Ejemplo 2 Regla 1

Recomendado	FF02:0000:0000:0000:0000:0000:0000:0001
Sin ceros iniciales	FF02: 0: 0: 0: 0: 0: 0: 1

Figura 11: Ejemplo 3 Regla 1

2. Omitir los segmentos Ceros, en esta segunda regla me permite reducir la notación de direcciones ipv6 con los puntos Dobles (::). Pueden remplazar cualquier cadena única y contigua de uno o más segmentos de 16 Bits.

Los puntos dobles se pueden utilizar solo una vez dentro de una dirección

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin ceros iniciales	2001: DB8: 0:1111: 0: 0: 0: 200
Comprimido	2001:DB8:0:1111::200

Figura 12: Regla 2

Ejemplos:

Recomendado	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Sin ceros iniciales	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Comprimido	FE80::123:4567:89AB:CDEF

Figura 13: Ejemplo 1 de Regla 2

Recomendado	FF02:0000:0000:0000:0000:0000:0000:0001
Sin ceros iniciales	FF02: 0: 0: 0: 0: 0: 0: 1
Comprimido	FF02::1

Figura 14: Ejemplo 2 de Regla 2

Recomendado	0000:0000:0000:0000:0000:0000:0000:0001
Sin ceros iniciales	0: 0: 0: 0: 0: 0: 0: 1
Comprimido	::1

Figura 15: Ejemplo 3 de regla 2

6.18 Longitud de Prefijo IPv6

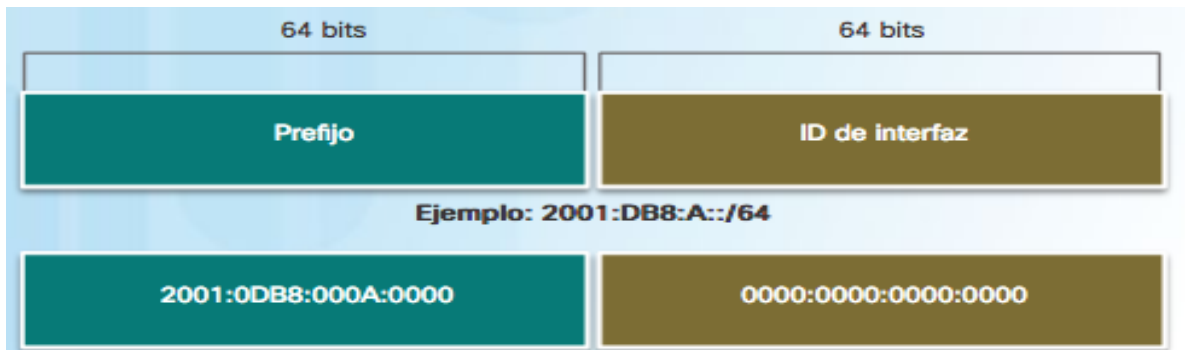


Figura 16: Longitud de prefijo IPv6

En la figura 16 representa el prefijo para una dirección IPv6 no utiliza la notación decimal punteada de mascara subred. La longitud de prefijo se utiliza para indicar la porción de red de una dirección IPv6 de la siguiente forma. Ipv6/longitud de prefijo.

La longitud de prefijo puede ir de 0 a 128. Para una red LAN la longitud es de 64 lo cual indica que los restantes 64 son para id de interfaz (porción de host) de la dirección.

6.19 Direcciones IPv6 de Unifusión

Este tipo de direcciones IPv6 identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Un paquete enviado a una dirección de unifusión es recibido para la interfaz que tiene asignada esa dirección.

Las direcciones IPv6 de origen deben ser direcciones de unifusión. Las direcciones de origen pueden ser de unifusión o multifusión. Las direcciones más conocidas como Unifusión son las globales y las direcciones link-local.

Unifusión Global

Las direcciones unifusión globales son similares a las direcciones públicas. Estas direcciones son enrutables entres los ISP proveedores de internet. Son globalmente exclusivas, estas direcciones se pueden configurar estáticamente o en forma dinámica.

Link Local

Este tipo de direcciones se utilizan para comunicarse con otros dispositivos en el mismo enlace local. El término “enlace” en IPv6 hace referencia a una Subred. Son exclusividad para ese enlace ya que no permite enrutar o avanzar del enlace. En otras palabras, los Routers no reenvían este tipo de direccionamiento en los paquetes a una dirección de origen o de destino link local.

Local Única

Este tipo de dirección es unificación local única. Tienen ciertas similitudes con las direcciones privadas **RFC1918** para IPv4. Pero existen grandes diferencias. Las direcciones locales únicas están en el rango **FC00::/7 a FDFF::/7**

Con las direcciones privadas IPv4 se podían combinar con NAT para proporcionar de varias a direcciones públicas. Esto lo hacen la mayoría de compañías para ocultar su red por seguridad.

Las direcciones locales únicas pueden usarse en dispositivos que no necesitan o nunca pueden acceder a otra red.

6.20 Estructura de una dirección IPv6 de Unificación global

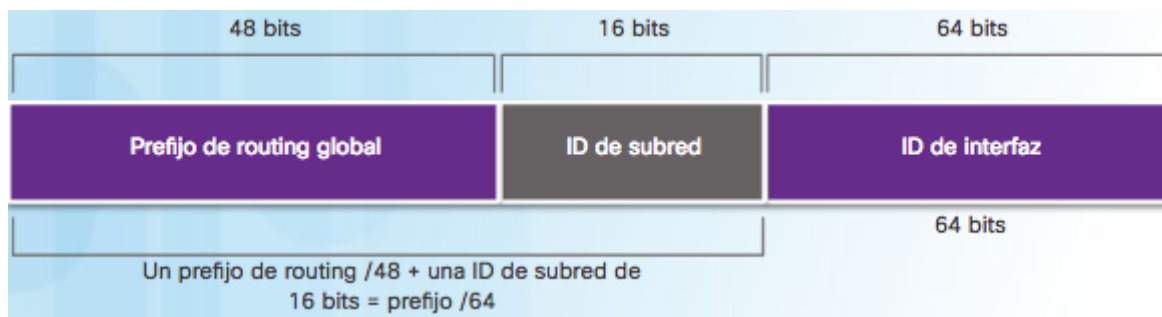


Figura 17: Dirección Global

Como anteriormente mencionamos este tipo de direccionamiento son globales únicas y enrutables por internet. La corporación de internet, para la asignación de nombres y números (ICANN). Operador de la IANNA, Asigna los bloques de direcciones a los 5 RIR.

Una dirección global IPv6 consta de tres partes:

- **Prefijo de Routing global**

Es la porción de red, la dirección que asigna el proveedor, por ejemplo, un ISP a sus clientes. Por lo general los RIR asignan un prefijo de Routing Global /48 son los más comunes.

El tamaño del prefijo de routing global determina el tamaño de la ID de subred.

- **ID de Subred**

Se utiliza el id de subred para identificar subredes dentro de su ubicación. Cuanto sea mayor es el ID de subred, se obtendrán más subredes disponibles.

- **ID de Interfaz**

Esta porción equivale a la de host, se utiliza “ID interfaz” debido que un host puede tener varias interfaces. Cada una o varias interfaces IPv6. Es recomendable especialmente usar subredes /64 en la mayoría de casos.

6.21 Direcciones Link Local Dinámicas

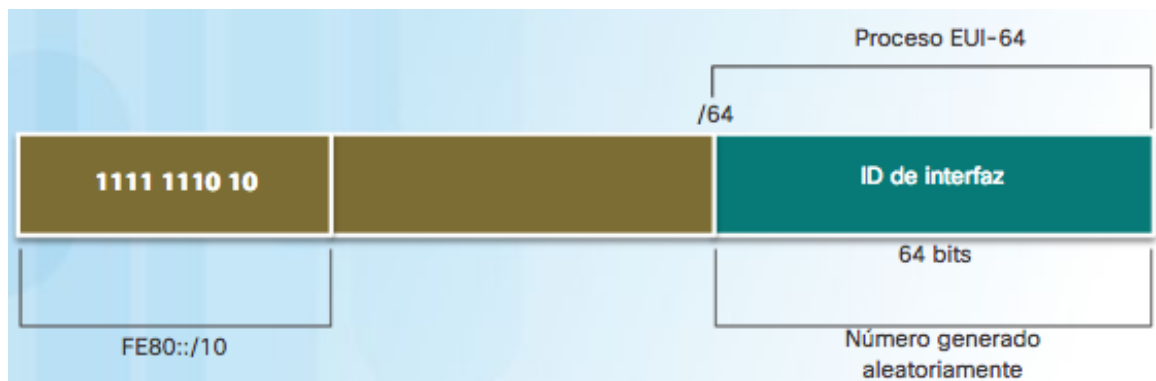


Figura 18: Dirección Link Local

Todos los dispositivos IPv6 deben tener una dirección link-local se pueden establecer dinámicamente o se puede configurar de forma manual.

Los Routers de cisco crean automáticamente una dirección IPv6 cada vez que se asigna una dirección de unificación global a la interfaz. Es dirección es única en ese enlace o red.

6.22 Direcciones Link-Local estáticas

Las direcciones link-Local estáticas se configuran manualmente para que sea una forma más fácil de recordar y llevar un control en cada enlace.

6.23 Protocolos de Routing IPv6

Los protocolos de enrutamiento para Ipv6 y funcionen correctamente depende tanto del Hardware como la versión de IOS para admitir IPv6 en sus interfaces.

Los protocolos compatibles son:

- RIPng (Rip de última Generación)
- OSPFv3
- EIGRP para Ipv6

6.24 Tipos de direcciones IPv6

Unifusión: Esta dirección identifica una interfaz de un dispositivo habilitado para IPV6. Siempre las direcciones de unifusion son de origen.

Este tipo de direcciones son de unifusión global, son parecidas a las direcciones IPV4 Publicas. Estas direcciones globales son enrutables por internet. Se pueden configurar estática o dinámicamente.

Multidifusión: Se utiliza para enviar un paquete a varios destinos de la red local.

Difusión por proximidad: es una dirección que se puede asignar a varios dispositivos. Un paquete enviado a una dirección unifusión por proximidad, se enruta al dispositivo más cercado.

6.25 Tecnología de Transición IPv4-IPv6

El IETF ("Internet Enginnering Task Force") está definido en la **RFC 4213**, creó diversos protocolos y herramientas para colaborar en esa transición y sea entendible para los administradores en realizar la migración a redes ipv6. Para J Walter Thompson analizando los métodos de transición en la RFC nos enfocaremos en el más compatible de acuerdo a la infraestructura a las aplicaciones que tienen actualmente.

Método Dual Stack

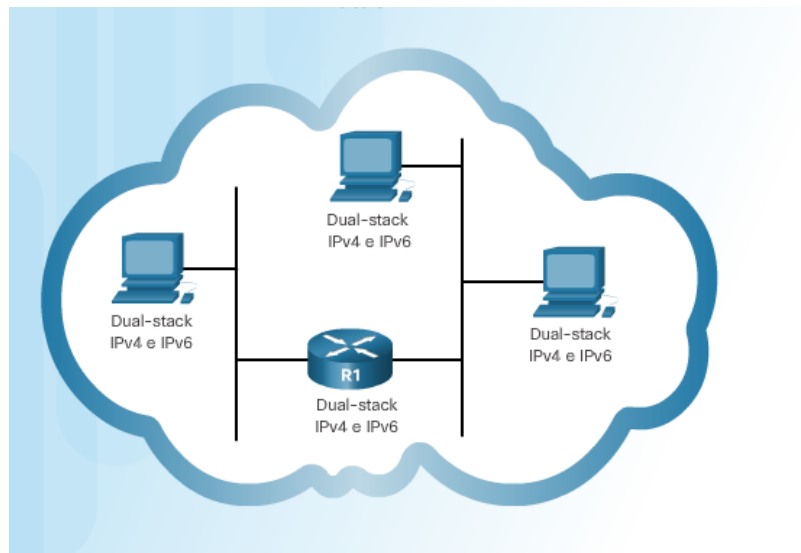


Figura 19: Dual Stack

Esta técnica de Dual Stack permite que IPV4 e IPV6 coexistan en el mismo método y en el mismo segmento de red. Los dispositivos de dual Stack ejecutan las pilas de protocolos de IPV4 e IPV6 simultáneamente. Este es un proceso suave. Se necesita una gran cantidad de direcciones ipv4 para desplegar las dos versiones en simultaneo en toda la red.

De esta forma, cuando se tenga un destino con Ipv4. Se utilizará el protocolo ipv4 y si el destino es ipv6 se utiliza el protocolo ipv6. Siempre de primeras irá ipv6 para empezar ir realizando la migración y tener la operación con la técnica durante un tiempo.

Es la técnica más fácil de utilizar para introducir IPv6 en una red. Que se describe en la RFC 2893. Cada nodo configurado con IPv4 e IPv6 por lo consiguiente las dos pilas de protocolo envían y reciben datagramas que pertenecen a ambos protocolos.

6.26 Tipos de túneles empleados como tecnologías de transición

1. 4in6

Encapsula el tráfico IPv4 en IPv6 (RFC2473).

2. 6in4-Tunelización

Como se muestra en la Figura # el protocolo de túnel es un método para transportar un paquete IPv6 en una red IPv4. El paquete se encapsula dentro de un paquete IPv4. (RFC4213).

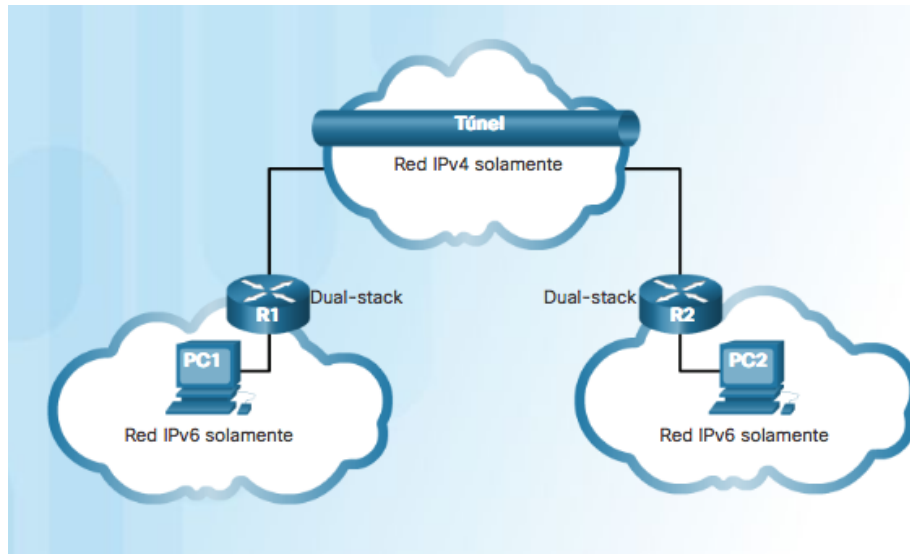


Figura 20: Tunelización

3. Traducción

En la figura 21, la traducción se refiere a traducciones de red 64 (NAT64) esto permite que los dispositivos habilitados para IPv6 se comuniquen con los dispositivos habilitados con IPv4 con la técnica de traducción similar a NAT para IPv4. Esto quiere decir que un paquete IPV6 se traduce a un paquete IPv4 y viceversa.

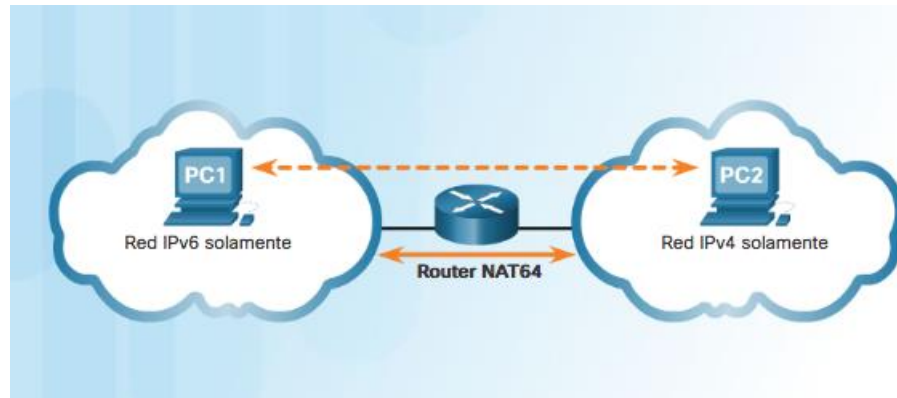


Figura 21: Traducción NAT64

4. Dual Stack Lite (DS-Lite)

Es un mecanismo que permite a un ISP no asignar direcciones IPv4 al cliente. Solamente entrega direccionamiento IPv6. El cliente puede escoger que rango privado le favorece más. Y viaje por la red del proveedor, encapsulando el paquete IP con IPv6 (RFC633).

7. Ingeniería del proyecto

7.1 Descripción de la situación actual

Construir un plan de diagnóstico que es el pilar fundamental de la transición. Es realizar una evaluación previa de la infraestructura, con el fin de conocer si es viable la adopción de ipv6 en la compañía J Walter Thompson. Actualmente tiene asignado un bloque direccionamiento ipv4 y obtiene un rango de direccionamiento para sus hosts. Pero el área IT conociendo que su infraestructura en algún momento debe pasar al nuevo protocolo ipv6. Desean empezar a formular su plan de trabajo con el fin de conocer los pasos a seguir sin que la operación se vea afectada.

7.2 Requerimientos de la información

Realizaremos una descripción general de la red actual de la compañía. Donde se involucra toda la infraestructura para la transición, es clave para conocer debilidades y fortalezas frente a IPv6. Con el fin de evaluar el impacto de esta transición sobre los equipos de red (Switches, Routers), Equipos de usuarios finales. De igual manera conocer topología física, lógica y servidores que prestan el servicio de aplicaciones que funcionan sobre esa red.

7.2.1 Hardware y Software.

Todos los fabricantes de Hardware conociendo de mucho antes el cambio de protocolo IP, han implementado ipv6 en sus equipos, en sistemas operativos en Routers, Switches, y firewall. En la memoria flash del equipo se aloja el ios donde se puede actualizar con otra versión superior para corregir o activar alguna mejora para compatibilidad con ipv6.

Es importante analizar los componentes de la red. Es la parte central de nuestra comunicación. En la actualidad los equipos de comunicaciones de cisco están diseñados para realizar esta migración y son compatibles con Dual Stack y ipv6.

Versiones de IOS compatibles con IPV6

IOS 12.2(2)T, Switch, Routers y APS
IOS 7.2.1.101.0 Wireless LAN Controllers

7.2.2 DNS y DHCP

Este mecanismo también se puede activar en el servidor DHCP para utilizar sistemas de autoconfiguración Ipv6, en servidores DNS, Sistema de Nombres de Dominio utilizando Ipv4 o IPV6. El DNS debe permitir y manejar registros Ipv4 e IPV6 para coincidencias de nombres de hosts con sus IPS específicas.

7.2.3 Servicios y aplicaciones

Todo depende de la complejidad del montaje del servicio o aplicación. Los administradores deben plantear las mejores recomendaciones y soluciones de acuerdo a las necesidades para no interrumpir el servicio y lograr la transición al protocolo IPV6.

7.2.4 Inventario IT

Para llevar a cabo dicha transición de IPV6 se realizó un levantamiento de información de la infraestructura actual de comunicaciones de J Walter Thompson. Esto nos permite realizar un plan de trabajo con los pasos necesarios para dicha transición de una forma controlada. Validando sus componentes desde su topología de red lógica, física, hardware y de software.

En esta información recolectada se centró en toda el área de comunicaciones y sus equipos que la compone como es el caso del routers, Switch de Acceso, Core y APS) seguido de servidores físicos y virtuales de aplicaciones. Y por último el grupo de periféricos. (PCS, Computador portátil y demás dispositivos).

Diagrama de Red J Walter Thompson.

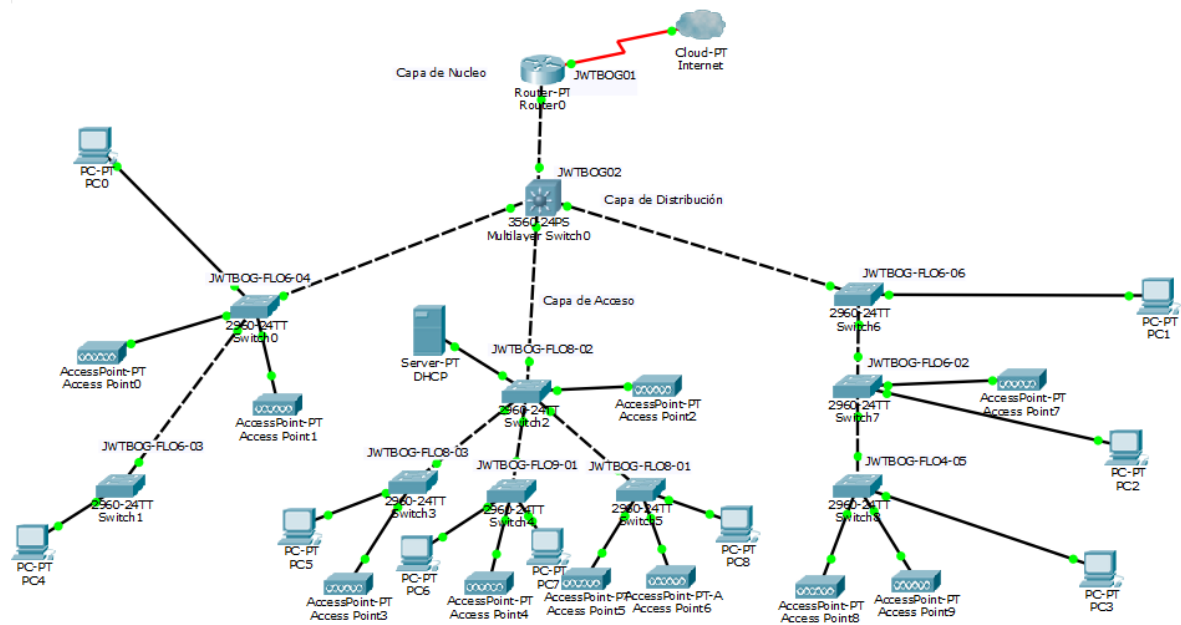


Figura 22: Diagrama de red

Inventario de Switches & Router

Nombre	Versión IOS	Referencia	Serial
JWTBOG01	15.7.3M2(ED)	ROUTER 3925	FTX1813AL8U
JWTBOG-FLO8-01	12.2(35)SE5	WS-3560G-48PS	FOC1217Y261
JWTBOG-FLO8-02	12.2(46)SE	C2960-LANBASEK9-M)	FOC1414Z3P7
JWTBOG-FLO8-03	12.2(46)SE	C2960-LANBASEK9-M)	FOC1414Z3PL
JWTBOG-FLO9-01	12.2.(25)SEE3	C2960-LANBASE-M)	FOC1130U2WT
JWTBOG-FLO6-02	12.2(46)SE	C2960-LANBASEK9-M)	FOC1414Z3P6
JWTBOG-FLO6-03	12.2.(25)SE5	WS-3560G-48PS	FOC1232Y13U
JWTBOG-FLO6-05	12.2.(25)SE5	WS-3560G-48PS	FOC1217Y25U
JWTBOG-FLO6-04	12.2.(25)SE5	WS-3560G-48PS	FOC1312Z2AC

Tabla 1: Inventario de Switches & Router

Inventario de APS

Piso	Nombre	Versión de IOS	Modelo
6	JWTBOG-FLO6-01	12.4(25e)JAM3	AIR-LAP1242AG-A-K)
5	JWTBOG-FLO5-02	12.4(25e)JAM3	AIR-LAP1242AG-A-K9)
6	JWTBOG-FLO6-02	15.2(2)JB3	C3500 (AP3G1-K9W8-M
6	JWTBOG-FLO6-06	15.2(2)JB3	C3500 (AP3G1-K9W8-M
6	JWTBOG-FLO6-03	15.2(2)JB3	C3500 (AP3G1-K9W8-M
5	JWTBOG-FLO5-01	12.4(25e)JAM3	AIR-LAP1242AG-A-K9)
7	JWTBOG-FLO7-01	12.4(25e)JAM3	AIR-LAP1242AG-A-K9)
6	JWTBOG-FLO6-04	15.2(2)JB3	AIR-CAP35021-A-K9
3	JWTBOG-FL03-02	12.4(25e)JAM3	AIR-LAP1242AG-A-K9)
3	JWTBOG-FL03-01	12.4(25e)JAM3	AIR-LAP1242AG-A-K9)
7	JWTBOG-FLO7-02	15.2(2)JB3	AIR-CAP35021-A-K9

Tabla 2: Inventario De APS

Inventario de Servidores

Server_Name	Business Application Hosted/supported	Operating System	Edition	Model	Serial Number	Memory	Total Cores	IPv4/IPv6
bog0ap01	Tango Condor	Windows Server. 2008 Standard	Estándar	Proliant DL380 G5	2UX74100GM	8gb	8 si	
bog0ap02	File Server / DHCP	Windows Server 2012 R2 Datacenter	Datacenter	Proliant DL380G6	2UX93801YL	6gb	4 si	
bog0ap04	Server Sophos	Windows Server 2008 R2 Standard	R2 Estándar	HP Pro 3130 MT	MXL0501D05	2gb	4 si	
bog0ap06	WebServer Tango	Windows Server 2008 R2 Enterprise		StorageWorks x1600	USE950N1GV	6gb	8 si	
bog0ap08	Sistema JWT	Windows Server 2008 R2 Standard	Estándar	BL460C G8	MXQ312016P	32gb	16 si	
bog0ap10	Tango Condor	Windows Server 2008 R2 Standard	Estándar	BL460C G8	MXQ3450FDX	64gb	32 si	
bog0fs02	File Server	Windows Server 2008R2	Estándar	Z600 WORKSTATION	2UA1071480	8gb	16 si	
bog0test11	Ambiente de pruebas Tango	Windows Server. 2008 Standard		HP Compaq 8000 Elite	MXJ947023M	3gb	4 si	
parson_file	File Server	Windows Server 2012 R2 Standard	Estándar	1650 Storage	USE5481182	16gb	6 si	
bog0filesglue02	File Server / Backups	Windows Storage Server 2008 R2 Estándar	Estándar	StorageWorks x1600 G2	USE253RK22	6gb	8 si	
med0fs01	File Server	Windows Storage Server 2008 Estandar	Estándar	HP Proliant SE1220	MXL0701D05	4gb	8 si	

Tabla 3: Inventario Servidores

7.3 Modelamiento del sistema

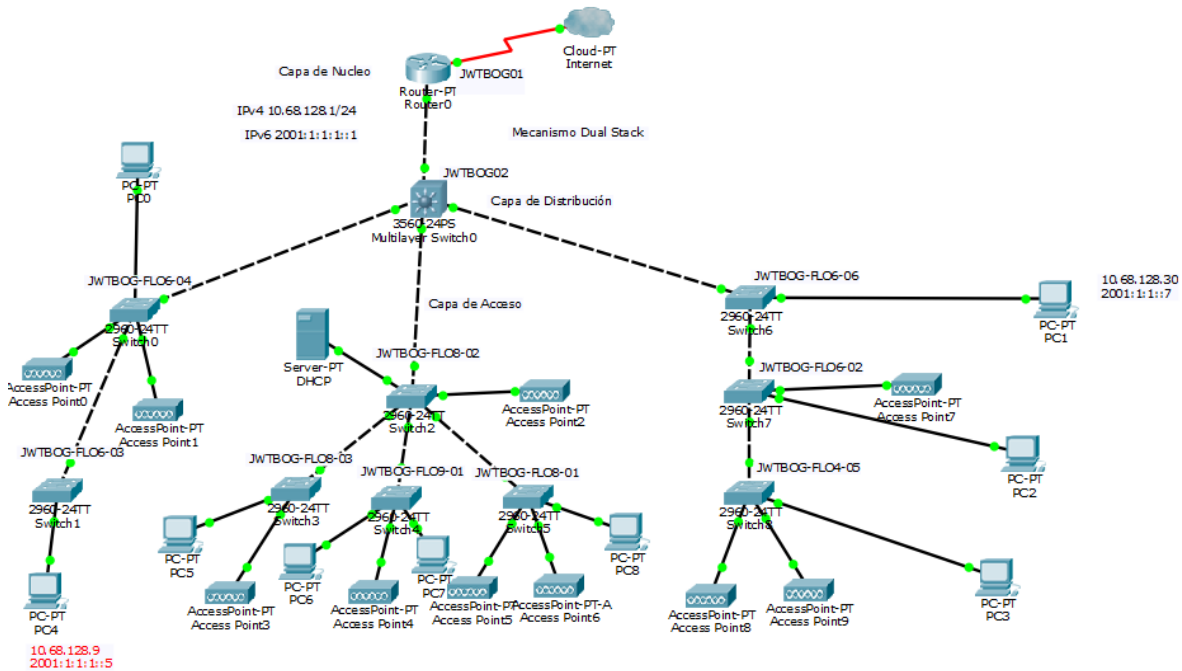


Figura 23: Modelamiento nueva configuración.

7.4 Descripción del sistema.

En este punto se realiza la configuración de Dual Stack para realizar pruebas con un simulador de Packet Tracer 7.0. De acuerdo a la información recopilada. Con el fin que los dos protocolos IPv4 e IPv6 trabajen juntos en esta transición.

La configuración de las interfaces en el router para el funcionamiento de los dos protocolos simultáneamente.

Router JWTBOG01

```
pv6 unicast-routing
interface FastEthernet0/0
ip address 10.68.128.1 255.255.255.0
duplex auto
speed auto
ipv6 address 2001:1:1:1::1/64
```

```
interface Serial1/0
ip address 10.2.2.1 255.255.255.0
ipv6 address 2001:7:7:7::1/64
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.68.128.1
ipv6 route ::/0 2001:1:1:1::1
```

Esta es una forma de configuración en el ios del router de cisco para habilitar interfaces y empezar a realizar comunicación con el proveedor ISP para pasar paquetes empaquetados IPv6 por la interfaz del proveedor.

Esto es un proceso de ir revisando las configuraciones actuales del cliente para definir la configuración correcta que debe llevar para que funcione el mecanismo de transición Dual Stack.

Este proceso debe trabajarse conjuntamente con el proveedor ISP.

8. Evaluación Económica del proyecto

8.1 Riesgo en fase de análisis

- Se analizó toda la información recopilada de la infraestructura que tiene actualmente el cliente. De esa manera conocer ventajas y desventajas en el momento en realizar la migración.
- Teniendo en cuenta el ítem anterior en el análisis se revisan características de aplicaciones, Switches, APS, Laptops, Desktops. Servidores, Topología física y lógica.
- En esta fase se revisó cuidadosamente toda la información recopilada de toda la infraestructura. Con el fin que cumpla tanto la parte de hardware y Software de cada dispositivo. De igual manera aplicaciones desarrolladas para la compañía y que actualmente están en producción.
- Se observó el diseño de la topología lógica y física para proponer el nuevo cambio implementando Dual Stack. Y como operarían todos los dispositivos soportando el nuevo protocolo Ipv6 y dejándolo como prioridad que Ipv4. De esta forma para ir desplazando al anterior protocolo y llegar al punto de dejar en funcionamiento solo Ipv6.
- Se evalúan todos los escenarios para obtener el mejor resultado óptimo en el momento de la migración y que sea muy transparente para todos los usuarios.

8.2 Riesgo en fase de Diseño

En esta fase se tomaron diferentes puntos de vista de los factores que podrían afectar el funcionamiento lógico.

- Se analizó el diseño lógico propuesto al cliente (JWT) en donde se plantea los aspectos de configuración y funcionamiento para dar a conocer su correcto funcionamiento. Teniendo en cuenta las necesidades del cliente y su infraestructura para lograr los mejores resultados.
- Se arranca desde el diseño que está actualmente con el fin de hacer unos cambios que no afecte la topología. Y para el área de IT sea un proceso muy transparente donde los cambios sean para beneficiar y sea un cambio positivo mejorar.

- El nuevo diseño lógico debe cumplir con la conectividad tanto interno como externo. Donde los paquetes lleguen desde su origen al destino. Implementando dual Stack permitirá que los dos protocolos de Internet puedan salir al exterior sin ningún inconveniente. Este nuevo cambio se debe realizar tanto en la parte interna como externa en este caso con el proveedor ISP para que habilite también en su enlace comunicación Ipv4 e IPv6.

8.3 Riesgo en fase de Codificación.

- En esta fase nos encontramos que en el momento de la migración y la operación esté activa, con los días se puede presentar un cambio para mejorar alguna necesidad del cliente que no se tuvo en cuenta y no se informó en el momento indicado.
- Por el tiempo de utilización de equipos de cisco se requiera renovar equipos y se necesita realizar migración de configuración a nuevos equipos.

8.4 Riesgo en fase de prueba.

En esta fase no se puede saltar ningún paso. En cada paso se debe verificar su funcionamiento, con el fin de alcanzar logro definido en este proyecto. El cual nos genera un buen desempeño, seguridad y eficacia frente al cliente J Walter Thompson.

- Se debe realizar un backup de las configuraciones anteriores de los dispositivos de cisco. Con el fin de efectuar los cambios necesarios y una vez realizadas las pruebas volver a la configuración anterior.
- Se revisa el desempeño de cada dispositivo en la configuración de Dual Stack. Verificando interfaces y conectividad. Esta prueba se realiza dejando unos equipos para verificar la funcionalidad. Luego se integra servidores y aplicaciones para monitorear comportamiento.
- Se solicita al área IT en realizar pruebas con un usuario donde se pueda integrar varias pruebas de conectividad, aplicaciones y demás servicios.
- Por último, se revisa que cada dispositivo de red como APS, laptops y servidores puedan obtener direccionamiento Ipv6 y tengan conectividad y enviar tráfico y tener un resultado óptimo en dichas pruebas.
- Las pruebas se basan en el levantamiento de información tanto en infraestructura como con el cliente. Con los principales cambios que se deben ejecutar para el correcto funcionamiento conociendo ventajas y desventajas que se puedan presentar.

8.5 Riesgo en fase de implementación.

En esta fase no se resalta muchos factores. Por el motivo que se realiza una fase de pruebas para realizar las configuraciones necesarias y se obtienen varios resultados donde se documenta que falló y cuál es su solución. En estas pruebas se refleja la funcionalidad del buen desempeño de conectividad y comunicación.

Una vez la fase de prueba tenga un porcentaje positivo se coordina fecha y hora de pasar la fase de prueba a producción. Teniendo los backups de respaldo por alguna eventualidad. Donde se monitorea la red para verificar desempeño de los dos protocolos en la red.

Estas actividades mencionadas anteriormente, están encaminadas a la habilitación del protocolo Ipv6 en cada uno de los componentes de Hardware y Software identificados en cada paso del proyecto y teniendo en cuenta el inventario entregado por IT de los activos que tienen actualmente en infraestructura por parte de J Walter Thompson.

8.6 Riesgo en fase de mantenimiento.

En esta fase de mantenimiento se pueden presentar factores de riesgo por eso se realizará revisión periódica y de realizar ajustes a la configuración si se requiere para mejorar.

Se analizará el comportamiento de los dispositivos de red, observando el consumo de recursos del equipo. Para saber si se está saturando con el fin de realizar dicho cambio y que esté operando con normalidad.

En esta fase también se tiene en cuenta el sistema operativo IOS si presenta problemas y no está funcionando correctamente para realizar el update o resetear el equipo de fábrica y luego subir la nueva versión para corregir dicho error.

9. Presupuesto Detallado

Este proyecto tiene una duración de 3 meses.

9.1 Costo de Infraestructura Física.

Tabla 4: costo1

Descripción	Cantidad	Costo unitario	Costo Total
Router Cisco	0	\$ 0	\$ 0
Switch Cisco	0	\$ 0	\$ 0
Laptop/PC	0	\$ 0	\$ 0
Equipos MAC	0	\$ 0	\$ 0
Servidores	0	\$ 0	\$ 0

De acuerdo a la información recopilada y entregada por el cliente. Se analizó y se llegó a la conclusión que no se necesita comprar un dispositivo adicional o cambiar equipos para dicha migración, porque la compañía cuenta con última tecnología que facilita realizar el proceso más sencillo.

9.1.1 Costo de implementación en Recursos Humanos.

Tabla 5: costo2

Descripción	Cantidad	Costo unitario	Costo Total
Sueldo Analista	1	\$ 12.200.000	\$ 12.200.000
Sueldo Especialista CCNA & CCNP	1	\$ 17.600.000	\$ 17.600.00

9.2 Costo Total del proyecto.

Costo Total x 3 meses.

Tabla 6: costo3

Descripción	Costo unitario	Costo Total
Infraestructura	\$ 0	\$ 0
Recurso Humano	\$ 29.800.00	\$ 29.800.000
Total	\$ 29.800.000	

10. Beneficios de Implementación.

10.1 Operación.

Lo primordial en esta implementación es: **la operación, la conectividad y los beneficios**. Son fundamentales para cualquier compañía. Por lo anterior se debe cumplir para nuestro cliente JWT. Es un gran paso a la migración por seguridad, y tener más equipos conectados.

Teniendo en cuenta que la operación seguirá operando con las dos versiones de protocolos Ipv4 e Ipv6. Se realizará la migración transitoria para alcanzar los objetivos planteados en este proyecto.

10.2 Gestión.

En la gestión se obtuvo beneficios en varios aspectos de la conectividad. Entre ellos está el área IT donde puede conectar muchos dispositivos en la red. Diseñar un mejor diagrama y planificar mucho mejor la entrega de direccionamiento a los hosts, servers, printers y Switches para obtener un control sobre ellos.

Tener mayor seguridad y obtener conectividad en cualquier parte del mundo. Otro beneficio es incluir telefonía voz IP. Esta transición ayuda a gestionar varias soluciones que se pueden llegar a necesitar más adelante. Conociendo que se tiene un protocolo, donde se obtienen varios beneficios que aportan nuevas mejoras.

10.3 Estratégico.

La compañía tendrá un beneficio en realizar su transición con tiempo y realizando todo el plan de trabajo con todos sus puntos. Más adelante en unos años se habilitará Ipv6 para todas las compañías y tendrán que realizarla en poco tiempo. Este es un beneficio de planificar algo que se vendrá a venir en unos años.

10.4 Infraestructura.

Al momento de realizar la transición contamos con la ventaja que tenemos equipos de Cisco que cumplen con esa función y genera un beneficio económico para la compañía. Un beneficio para el área IT que toda la infraestructura funciona para dicha migración, ya que es primordial contar con Hardware, Software con todo el levantamiento de información. Y adicional un beneficio para usuarios en conectar equipos autorizados en la red.

10.5 De IT.

La compañía tendrá varios beneficios en esta transición del protocolo IP. Que será trabajado con el grupo de ingeniería de la compañía JWT. Los beneficios Son: conocimiento de Topología actual, levantamiento de información, ¿por qué realizar el cambio? Costos, tiempo, capacitación y entrega de documentación. Con el fin de dejar una documentación precisa y clara al departamento de IT. Para futuros cambios si se llega a necesitar.

11. Cronograma


		Nombre de tarea	Duración	Comienzo	Fin
1		Revisión de Infraestructura fisica	2 días	lun 06/11/17	mar 07/11/17
2		Revisión de configuración de Router	1 día?	mié 08/11/17	mié 08/11/17
3		Revisión de diseño de Topologia logica y Fisica	1 día?	jue 09/11/17	jue 09/11/17
4		Inventario General de sistemas	3 días	vie 10/11/17	mar 14/11/17
5		Reunión Area IT sobre inventario	1 día	mié 22/11/17	mié 22/11/17
6		Reunión IT sobre IPV6 y ventajas de la migración.	1 día	jue 23/11/17	jue 23/11/17
7		Se entregará documento del proyecto a desarrollar	1 día	lun 11/12/17	lun 11/12/17
8		Puntos a revisar del proyecto.	1 día	mar 12/12/17	mar 12/12/17
9		Revisión de la infraestual actual para la migración.	1 día	mar 12/12/17	mar 12/12/17
10		Pasos a seguir para la migración	1 día	vie 15/12/17	vie 15/12/17
11		Presupuesto para dicha migración	1 día	mar 19/12/17	mar 19/12/17
12		Personal encargado para la migración.	1 día	mar 19/12/17	mar 19/12/17
13		Revisar configuración de Router y Switches	2 días	mar 09/01/18	mié 10/01/18
14		Revisión de aplicaciones y funcionamiento	1 día	vie 12/01/18	vie 12/01/18
15		Reunión para validar Días tentativos para pruebas	1 día	vie 23/02/18	vie 23/02/18
16		Fase de prueba	2 días	vie 09/03/18	dom 11/03/18
17		Se realiza copia de seguridad de la configuración	2 días	vie 09/03/18	dom 11/03/18
18		Se procede a realizar nuevas configuraciones	2 días	vie 09/03/18	dom 11/03/18
19		Se valida configuración y se verifica funcionamiento	2 días	vie 09/03/18	dom 11/03/18
20		se devuelve el cambio	2 días	vie 09/03/18	dom 11/03/18
21		Se toman apuntes de acuerdo al comportamiento.	2 días	vie 09/03/18	dom 11/03/18
22		Se necesita un fin de semana para validar los camb	1 día	sáb 17/03/18	sáb 17/03/18
23		Se monitorea los cambios	1 día	sáb 17/03/18	sáb 17/03/18
24		Se verifica fechas de migración.	1 día	mié 21/03/18	mié 21/03/18
25		Se envia el plan de trabajo a otra área de soporte de	5 días	mié 04/04/18	mar 10/04/18

Figura 24: Cronograma

12. Recomendaciones

- En la actualidad varias redes están trabajando aun con el protocolo Ipv4, y solo entidades públicas del gobierno están migrando al nuevo protocolo Ipv6 de acuerdo a la información suministrada por las TIC. (Tecnologías de la información y la comunicación).

Estas entidades ya están trabajando en ello para realizar todas las pruebas e ir conociendo las nuevas características propias del nuevo protocolo y con ellas realizar una buena planificación en el momento de la transición.

- Uno de los primeros pasos es conocer muy bien su infraestructura tanto física como lógica, también tener un buen inventario de dispositivos tanto de hardware, software y aplicaciones que estén utilizando en la actualidad. De esta forma empezaremos a organizar nuestro plan de trabajo para obtener una buena migración.
- Tener presente que antes de realizar una migración en nuestras redes y cualquier otro tipo de cambio es necesario planificarlas y realizar las pruebas correspondientes. Debemos seguir ciertos pasos y siempre realizar un backup de las configuraciones actuales por si es necesario devolvernos para corregir algún error.
- Es importante hablar con el proveedor ISP para comentarles de la transición que se va realizar en la red de la compañía y adicional los cambios que ellos tienen que hacer al Router para permitir el tráfico IPv4 e IPv6.
- Se debe realizar una planificación, Con el fin de tener una topología lógica de los dos protocolos IPv4 e IPv6 para saber cómo será la asignación de direcciones IPv6 en la red y tener un control. Y conocer que direcciones serán asignada a los servidores y dispositivos de comunicaciones.

13. Conclusiones

- Las redes como es internet desempeña un papel importante en cualquier compañía. Sea pequeña, mediana o grande. Por eso debemos contar con una estructura adecuada y un equipo de trabajo IT que pueda ir mejorando de acuerdo a su experiencia y conocimientos en el área de telecomunicaciones para suplir cualquier necesidad del cliente.
- Se ha presentado un incremento de demanda de direcciones ipv4, debido al crecimiento de dispositivos y aplicaciones que utilizan este tipo de direccionamiento. Se ha presentado el agotamiento y en los siguientes años será muy importante que la gran mayoría de compañías empiecen su migración y no estar corriendo en dicha migración. es importante tomarse su tiempo para realizar un análisis de tiempo, solventar los posibles inconvenientes y gastos que se pueden presentar.
- La seguridad es una ventaja que nos brinda en la capa tercera de red en el modelo OSI. El protocolo Ipsec se vuelve obligatorio. De esa manera tener infraestructura y aplicaciones seguras.
- Todos los fabricantes de equipos de cómputo, cisco y Windows. En la actualidad ya tienen todo el soporte necesario para migrar todos sus equipos y sistemas operativos tanto de Windows, Linux, Macintos, ios de cisco. Ya están preparados para la transición, con una buena planificación se logrará pasar al nuevo protocolo Ipv6.
- Para realizar esta migración se debe realizar todos los pasos necesarios. Con el fin de realizar una correcta migración sin excluir las pruebas en cada paso. Para obtener la transición adecuada y planteada.

14. Bibliografía

1. NAVARRO, Anna. **Diccionario de términos de comunicaciones y redes.** España: cisco press,2003.600 pp.
2. O'FLAHERTY, Christian. **IPv6 para todos- 1ª edición-** Buenos Aires: Asociación Civil Argentinos en internet, 2009.
3. E. BRICEÑO, José. **Transmisión de datos** - 3ª edición – Venezuela: universidad de los andes Facultad de ingeniería, 2005

Webgrafía

1. Cisco systems Inc. **“IPv6 configuration Guide, cisco IOS Release 15.2MT”**. {En línea}. {17 agosto de 2017} disponible en: (<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book.pdf>).
2. Lacnic **“Acerca de Lacnic”** {En Línea}. {17 agosto de 2017} disponible en: (<http://www.lacnic.net/966/1/lacnic/acerca-de-lacnic>).
3. Ietf. Network Working group. **“Internet protocol, versión 6 (IPv6) especification”** {En Línea}. {22 agosto de 2017} disponible en: (<http://www.ietf.org/rfc/rfc2460.txt?number=2460>).
4. Ietf. Network Working group. **“Transition mechanisms for IPv6 hosts and Routers”** {En Línea}. {22 agosto de 2017} disponible en: (<https://www.ietf.org/rfc/rfc2893.txt>).
5. Cisco systems Inc., **“Cisco Networking Academy, is an IT skills and career building program available to learning institutions and individuals worldwide”** {En Línea}. {Años 2017 y 2018} disponible en: (<https://www.netacad.com/>)
6. Ietf. Network Working group. **“IP Autentication Header”** {En Línea}. {22 de agosto de 2017} disponible en: (<https://www.ietf.org/rfc/rfc4302.txt?number=4302>)
7. Lacnic. **“Mecanismos de transición”** {En línea}. {23 de agosto 2017} disponible en: (<http://portalipv6.lacnic.net/mecanismos-de-transicion/>)
8. Cisco systems Inc. **“Configure dual Stack IPv6”** {En Línea}. {23 de agosto de 2017} disponible en: (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_0_1/sysConfig/CUCM_BK_C733E983_00_cucm-system-configuration-guide/configure_dual_stack_ipv6.pdf)