INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECANICA Y ELECTRICA

UNIDAD PROFESIONAL “ADOLFO LOPEZ MATEOS”

INGENIERIA EN COMUNICACIONES Y ELECTRONICA

“**Transición de IPv4 a IPv6 usando el método Doble Pila**”

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMUNICACIONES Y ELECTRONICA

PRESENTAN:

Barrera León Ivonne

García Uribe Pedro Roberto

Saldaña Vargas Moritz Oswaldo

ASESORES:

M. en C. José Ernesto Rojas Lima

M. en C. Pedro Gustavo Magaña del Río

MEXICO, D.F. 2015

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS"

TEMA DE TESIS

QUE PARA OBTENER EL TITULO DE INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

POR LA OPCIÓN DE TITULACIÓN **TESIS COLECTIVA V EXAMEN ORAL INDIVIDUAL**

DEBERA (N) DESARROLLAR

C. IVONNE BARRERA LEON
C. PEDRO ROBERTO GARCIA URIBE
C. MORITZ OSVALDO SALDAÑA VARGAS

"TRANSICIÓN DE IPV4 A IPV6 UTILIZANDO EL MÉTODO DOBLE PILA"

UTILIZAR EL MÉTODO DE DOBLE PILA QUE PERMITA LA COEXISTENCIA ENTRE IPV4 E IPV6

- INTRODUCCIÓN
- ANTECEDENTES
- MODELOS DE REFERENCIA TCP/IP Y OSI
- PROTOCOLOS DE INTERNET IPV4 E IPV6
- PROTOCOLOS DE ENRUTAMIENTO
- DESARROLLO DEL PROYECTO
- RESULTADOS
- CONCLUSIONES
- ANEXOS
- ACRÓNIMOS
- BIBLIOGRAFÍA

MÉXICO D.F. A 22 **DE SEPTIEMBRE** DE 2014.

A S E S O R E S

INC. JOSE **ERNESTO ROJA** SLIMA

ING. PEDRO GUSTAVO MAGANA DEL RIO

ING. **PATRICIA LORENA RAMIREZ RANGEL**
JEFE DEL DEPARTAMENTO DE
INGENIERA EN COMUNICACIONES Y ELECTRONICA

DEDICATORIA

La presente tesis la dedico a mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo, a mi hijo y su papá que han sido mi mayor motivación, resaltando también todo el apoyo de mis maestros. Todo este trabajo ha sido posible gracias a ellos.

IVONNE

DEDICATORIA

A mis Padres a quienes dedico este sueño que se ha completado gracias a su esfuerzo y al apoyo que me brindaron durante mi carrera profesional y por enseñarme a ser el gran ser humano que ahora soy, esto es para ustedes con todo mi amor y mi esfuerzo gracias.

A mis dos hermanas que me dieron todo su apoyo y sus sabias palabras que me daban fuerza y ánimo para terminar este gran proyecto.

A mis Abuelos quienes vieron el inicio de mi carrera a ellos que ahora no se encuentran aquí, pero sé que siempre estuvieron a mi lado apoyándome y brindándome todo su amor y sus fuerzas para terminar esta etapa de mi vida para ustedes con todo mi amor.

A mis amigos de la ESIME quienes siempre me apoyaron y confiaron en mí gracias.

PEDRO ROBERTO

AGRADECIMIENTOS

Al Instituto Politécnico Nacional por brindarme todos los conocimientos y por formarme como un gran profesionista para que pueda ser un excelente ciudadano capaz de resolver los problemas a los que me enfrente y ser útil para mi país.

A mis asesores M. en C. José Ernesto Rojas Lima y al Ing. Pedro Gustavo Magaña del Río quien nos brindaron todo su apoyo y su conocimiento para poder concluir con este proyecto, por habernos dedicado de su tiempo para aclararnos nuestras dudas por hacer que este proyecto quedara excelente a ustedes muchas gracias.

Al M. en C. Roberto Muñoz Castro quien nos apoyó y nos dio la oportunidad de trabajar a su lado en la instalaciones de la Dirección de Computo y Comunicaciones a usted que tanto apoyo nos brindó muchas gracias sin su ayuda esto no hubiera sido posible.

Al Ing. Julio Delgado Pérez que gracias a su amplio conocimiento en Redes no ayudo para resolver nuestras dudas y apoyarnos en la revisión de nuestra tesis muchas gracias.

Y finalmente a la ESIME que gracias a ella ahora soy un ingeniero formado por grandes profesores quienes me brindaron su conocimiento, orgulloso de pertenecer a esta gran institución.

PEDRO ROBERTO

DEDICATORIA

A MIS PADRES

Quienes me han heredado el tesoro más valioso que pueda dársele a un hijo: amor.
Quienes sin escatimar esfuerzo alguno, han sacrificado gran parte de su vida.
Me han formado y educado.
A quienes la ilusión de su existencia a sido convertirme en persona de provecho.
A quienes nunca podre pagar todos los desvelos ni con las riquezas más grandes del mundo.
Y a Dios le agradezco eternamente la dicha de tener unos padres como ustedes.
Hoy y siempre gracias por lo que juntos hemos logrado.

MORITZ OSWALDO

O B J E T I V O

Utilizar el método de doble pila que nos permita la coexistencia entre IPv4 con IPv6.

INTRODUCCION

El intercambio de información entre dos entidades debe de realizarse en forma totalmente transparente de tal forma que dicha información alcance el destino adecuado independientemente de la ubicación física del equipo que se utiliza. Al convivir los equipos con una multiplicidad de ellos interactuando en una red como internet, un aspecto que cobra importancia radical es la identificación única de cada uno de los equipos, lo cual es la base para el envío y recepción de la información; esa identificación única es conocida como dirección.

Existen modelos que cuentan con funciones que se encargan de llevar la información desde su origen hasta su destino a través del descubrimiento de trayectorias especificas entre la multiplicidad de equipos que se encuentran interconectados.

Para que dos equipos tengan una interacción entre si se necesita de una comunicación y un medio los cuales sean entendibles para ambos, para poder así entablar un intercambio de información.

Dichas comunicaciones están apoyadas de ciertos protocolos que se encargan de hacer una traducción para que la información pueda viajar entre varios dispositivos conectados a una red.

ANTECEDENTES

Es muy importante la coexistencia de los ambientes tradicionalmente desarrollados utilizando IPv4, los cuales constituyen y enmarcan la gran mayoría de redes tanto públicas como privadas a nivel mundial; esta coexistencia y transparencia de información debe ser proporcionada a las nacientes estructuras IPv6, con redes de diversa naturaleza que no pueden sustraerse de la convivencia de las ya existentes debido al intercambio de los datos de los múltiples usuarios de las redes existentes y de las de reciente creación.

Debido al agotamiento de las direcciones IPv4 es necesario pensar en algún método que permita la coexistencia entre dichas estructuras, para ello contamos con ciertos mecanismos de transición los cuales permiten una compatibilidad entre ambos protocolos.

Gracias a los métodos de transición puede existir una convivencia entre ambos protocolos, haciendo esto una posibilidad para no presentar problemas futuros de agotamiento de direcciones y empezar a crear una estabilidad para que IPv6 pueda ser implementado de una manera eficiente.

Índice

INTRODUCCIÓN

ANTECEDENTES

Capítulo 1

Modelos de Referencia TCP/IP y OSI

1.1.- Comunicación de datos a través de redes

1.1.1 Redes de área amplia……...16
1.1.2 Redes de área local……17

1.2.- Conceptos básicos de los protocolos de comunicación de datos

1.2.1 Características……18

1.2.2 Funciones……..…...20

1.2.3 Arquitecturas……...22

1.3.- Modelos de referencia TCP y OSI

1.3.1 Arquitectura de protocolos TCP/IP……...….22

1.3.2 Modelo OSI…….22

1.3.3 Comparativa……31

Capítulo 2
Protocolos de Internet IPv4 e IPv6

2.1 Características principales de IPv4……..34

2.1.1 Clases de direcciones……35

2.1.2 Cabecera del Protocolo IPv4……38

2.2 Restricciones del protocolo IPv4……40

2.2.1 Problemática principal en IPv4……40

2.2.2 Esfuerzos de conservación en IPv4……41

2.3 Protocolo de internet versión 6……42

2.3.1 Características principales de IPv6……42

2.3.2 Formato general de un datagrama IPv6……43

2.4 Formato de la cabecera IPv6……44

2.4.1 Descripción de los campos de la cabecera de IPv6……45

2.4.2 Cabecera de extensión de IPv6……47

2.4.3 Descripción de los campos de extensión de la cabecera……48

2.5 Direccionamiento en IPv6……52

2.6 Comparación entre IPv4 e IPv6……55

Capítulo 3
PROTOCOLOS DE ENRUTAMIENTO

3.1.- Principios Básicos de Enrutamiento……57

3.1.1.- Métrica de Enrutamiento……57

3.1.2.- Distancia administrativa……..59

3.1.3.- Tablas de enrutamiento……...60

3.2.- Protocolos enrutados……..……..61

3.3.- Protocolos de enrutamiento..……64

3.3.1.- Vector distancia…….65

3.3.2.- Esta de enlace……...67

3.4.- Enrutamiento Estático y Dinámico……..……69

3.5.- Bucles de enrutamiento…….....……...70

Capitulo 4
DESARROLLO DEL PROYECTO

4.1.- OSPF……73

4.1.1.- Funcionamiento……74

4.1.2.- Algoritmo OSPF Dijkstra (DIJK59)……83

4.2.- Coexistencia entre IPv4 e IPv6…..……..85

4.2.1.- Método Doble Pila……85

4.2.2.- Ventajas del modelo Doble pila……..88

4.2.3.- Problemas Doble Pila……...89

4.3.- Resultados……89

4.3.1.- Diagrama de la Red……90

4.3.2.- Configuración de Enrutadores y Tablas de Enrutamiento……...92

4.3.3.- Prueba de Ping…….....95

4.3.4.- Obtención de Métricas de Enrutamiento…….....97

4.4.- Problemas……100

Conclusiones……104

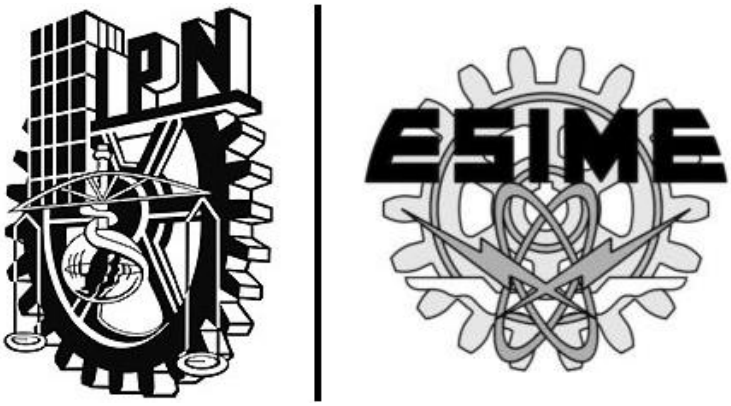
Bibliografía……106

Acronimos……..108

Apéndice……110

Wireshark……...…111

Código de configuración de los Routers……...114



CAPÍTULO 1 | “Modelos de Referencia TCP/IP y OSI

Capítulo 1: Modelos de Referencia TCP/IP y OSI

1.1.- Comunicación de datos a través de redes

El objetivo principal de todo sistema de comunicación es intercambiar información entre dos entidades (dispositivos). Los elementos clave en este tipo de sistema son los siguientes:

- **Fuente:** Este dispositivo genera los datos a transmitir: por ejemplo teléfonos o computadores personales.
- **Transmisor:** Normalmente los datos son generados por la fuente, estos no se transmiten directamente tal y como son generados. Al contrario, el transmisor transforma y codifica la información, generando señales electromagnéticas susceptibles de ser transmitidas a través de algún sistema de transmisión. Por ejemplo un MODEM convierte las cadenas de bits generadas por una computadora y las transforma en señales analógicas que pueden ser transmitidas a través de la red.
- **Transmisión de datos:** Puede ser desde una sencilla línea de transmisión hasta una compleja red que conecta la fuente con el destino.
- **Receptor:** Acepta la señal que proviene del sistema de transmisión y la transforma de tal manera que pueda ser manejada por el dispositivo destino.
- **Destino:** Toma los datos del receptor, es decir recibe la información de la compuerta de enlace enviada de la fuente.

Basado en lo anterior, y si se requiere comunicarse con un equipo ubicado en un área no cercana se requiere tomar en cuenta lo siguiente:

Una de las soluciones a este problema es conectar cada dispositivo a una red de comunicación, existen varias categorías de redes pero se enfocará en dos, las cuales son: Redes de Área Amplia (WAN, por sus siglas en inglés, Wireless Area Network) y las Redes de Área Local (LAN, por sus siglas en inglés, Local Area Network), las cuales se explicarán a continuación.

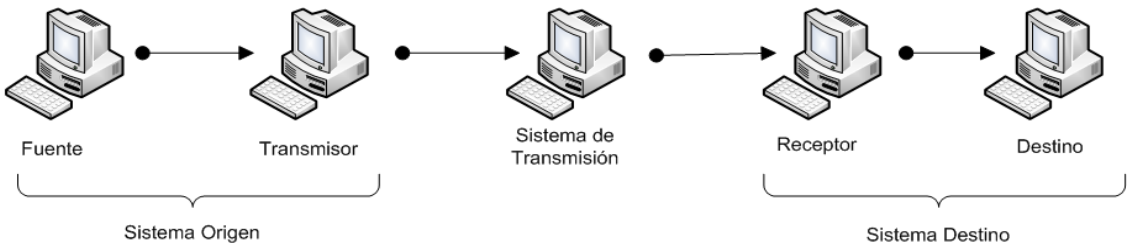


Figura 1.1 Comunicación de Datos

1.1.1.- Redes de Área Amplia (WAN)

Son aquellas que abarcan una gran área geográfica, con frecuencia un país o un continente, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Típicamente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos no les interesa el contenido de los datos, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

Tradicionalmente, las WAN se han implementado usando una de las dos tecnologías siguientes: conmutación de circuitos y conmutación de paquetes.

Conmutación de circuitos

En las redes de conmutación de circuitos se establece a través de los nodos de la red un camino dedicado a la interconexión de dos estaciones. El camino es una secuencia de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan o conmutan por el canal apropiado de salida sin retardos.

Conmutación de paquetes

En este caso no es necesario hacer una reserva a priori de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo a nodo en la red siguiendo algún camino entre la estación origen y el destino. En cada nodo, el paquete se recibe completamente, se almacena durante un intervalo breve y posteriormente se pasa al siguiente nodo.

Las redes de conmutación de paquetes se usan fundamentalmente para comunicaciones terminal-computador y computador-computador.

En la Figura 1.2 se muestra una red WAN.

Figura 1.2 Alcance de una red WAN

1.1.2.- Redes de Área Local

Al igual que las redes de área amplia, una red de área local es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para

El intercambio de información entre ellos. Las redes de área local son redes de área privada es decir cubren un área geográfica pequeña, se encuentran en un solo edificio o en un campus de poca longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en una oficina para compartir información, recursos (por ejemplo, impresoras).

Tradicionalmente, en LAN se utiliza la difusión en lugar de utilizar técnicas de conmutación. En una red de difusión, no hay nodos intermedios. En cada estación hay un transmisor/receptor que se comunica con las otras estaciones a través de un medio compartido.

Una transmisión desde cualquier estación se recibirá por todas las otras estaciones. Los datos se transmiten en forma de paquetes. Debido a que el medio es compartido, en cada instante de tiempo solo una estación podrá transmitir el paquete.

1.2.- Conceptos de los Protocolos de Comunicación de Datos

Para reducir la complejidad de su diseño, la mayoría de las redes está organizada como una pila de capas o niveles, cada una construida a partir de la que está debajo de ella. El número de capas, así como el nombre, contenido y función de cada una de ellas difieren de red a red. El propósito de cada capa es ofrecer ciertos servicios a las capas superiores.

La capa n de una máquina mantiene una conversación con la capa n de otra máquina. Las reglas y convenciones utilizadas en esta conversación se conocen de manera colectiva como protocolos de capa. Básicamente un protocolo es un acuerdo entre las partes de comunicación sobre cómo se debe llevar a cabo la comunicación.

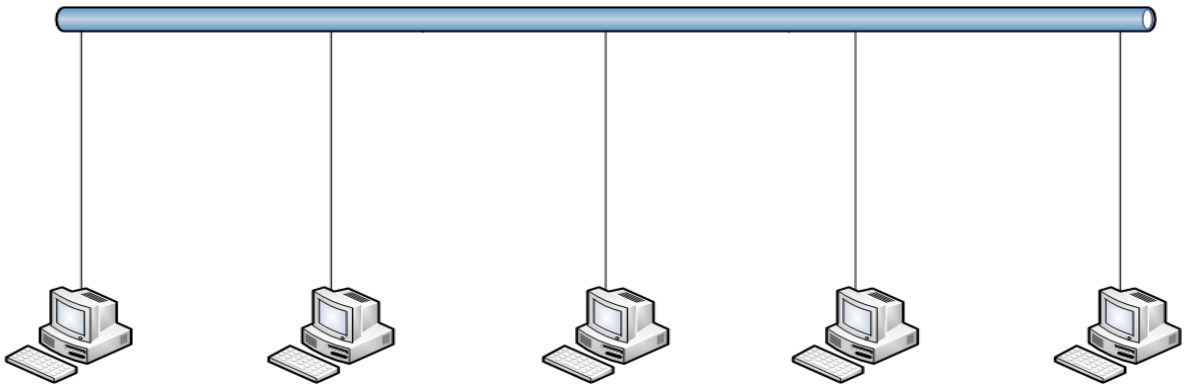
1.2.1.- Características

Los protocolos se caracterizan fundamentalmente por ser:

- Directos/indirectos
- Monolíticos/estructurados
- Simétricos/asimétricos
- Estándares/ no estándares

La comunicación entre dos entidades puede ser **directa** o **indirecta.** Si los dos sistemas que se van a comunicar comparten una línea punto a punto, las entidades de estos sistemas se podrán comunicar directamente; es decir, los datos y la información de control pasarán directamente entre las entidades. Esta misma idea es aplicable a configuración multipunto aunque en este caso la entidad deberá solucionar el problema de control de acceso. Si los sistemas se conectan a través de una red conmutada no se podrá aplicar un protocolo directo. El posible intercambio de datos entre dos entidades dependerá a su vez del buen funcionamiento de otras entidades. En la figura 1.3 se describen algunas situaciones posibles.

(a) Punto a Punto



(b)Red de difusión Multipunto

Figura 1.3 Tipos de conexión en un sistema de comunicación

Otra característica de los protocolos es su carácter **monolítico** o **estructurado**. En un protocolo monolítico hay un único protocolo que se encarga de todas las funciones de comunicación desde la conexión física a la red, hasta la lógica para dividir los mensajes a transmitir en paquetes.

Un protocolo estructurado consiste en un conjunto de protocolos organizados con una estructura por capas o jerárquica. Las funciones básicas se implementarán en las entidades de los niveles inferiores, las cuales proporcionan servicios a las entidades de los niveles superiores.

Un protocolo puede ser **simétrico** o **asimétrico** en ciertas situaciones la simetría vendrá impuesta por la naturaleza del intercambio (por ejemplo, un proceso <<cliente>> y un <<servidor>>), o por la necesidad de reducir la complejidad de las entidades o los sistemas.

Un protocolo puede ser **estándar o no estándar**. El no estándar es aquel que se diseña y se implementa para una comunicación particular, o al menos para un ordenador con un modelo particular. Y el estándar se implementa para una comunicación bastante organizada la cual requiere de una serie de estándares para poder llevarse a cabo.

1.2.2.- Funciones

Las funciones de los protocolos se pueden clasificar dependiendo a lo que realicen pues no todos pueden tener las mismas funciones ya que ello implicaría una duplicación innecesaria de las mismas. No obstante, hay algunas funciones que se repiten en ciertos protocolos situados en distintos niveles.

Las funciones de un protocolo se pueden agrupar en:

- Encapsulamiento
- Segmentación y ensamblado
- Control de la conexión
- Entrega en orden
- Control de flujo
- Control de errores
- Direccionamiento
- Multiplexaje
- Servicios de transmisión

Encapsulamiento: Se denomina encapsulamiento al hecho de añadir a los datos información de control. Los datos se aceptan o se generan por una entidad, y se encapsulan en la Unidad de Datos de Protocolo (PDU, por sus siglas en inglés, Protocol Data Unit) junto con la información de control.

Estas se utilizan para el intercambio de datos entre unidades heterogéneas.

Segmentación y ensamblado: Se denomina segmentación al hecho de enviar una cadena de datos agrupados en forma de mensaje (comprimir información) pero los protocolos de los niveles inferiores pueden necesitar partir los datos en bloques más pequeños. El procedimiento contrario a la segmentación se denomina ensamblado, donde los datos segmentados tendrán que ensamblarse recuperando el formato de los mensajes originales para entregarlos a la entidad de aplicación destino.

Control de la conexión: Se puede definir la trasferencia orientada a conexión como aquella en que dos extremos numeran y controlan las PDU tanto de entrada como de salida. La característica principal de la trasferencia orientada a conexión es que cada extremo numera secuencialmente las PDU que envía al otro extremo.

Entrega en orden: Si dos entidades de comunicación residen en estaciones, diferentes conectadas a través de un red, habrá un cierto riesgo de que las PDU lleguen con un orden diferente al de partida ya que puede haber rutas diferentes para llegar al destino, lo que puede impedir la llegada en orden.

Control de Flujo: Es una operación realizada por la entidad receptora para limitar la velocidad o cantidad de datos que envía la entidad emisora. La aproximación más sencilla para el control del flujo es el procedimiento de parada-y-espera, en el que cada PDU se debe confirmar antes de que se pueda enviar la siguiente.

Control de errores: Las técnicas del control de errores son necesarias para recuperar pérdidas o deterioros de los datos y de la información de control. Generalmente el control de errores se implementa mediante 2 funciones separadas la detención de errores y la retransmisión. Para llevar a cabo la detección, el emisor inserta en cada PDU transmitido un código que sea capaz de detectar errores, este código será función de los bits que constituyan la PDU. El receptor comprobará el valor del código en la PDU recibida. Si se detecta un error, el receptor descarta la PDU.

Direccionamiento: Hace referencia al nivel de la arquitectura de comunicaciones en el que se identifica a la identidad. Normalmente cada sistema o sistema intermedio está asociado a una única dirección: Esa dirección por lo general es una dirección del nivel de red. También denominada dirección de Internet (IP, por sus siglas en inglés, Internet Protocol). La dirección del nivel de red se utiliza para encaminar los PDU a través de la red o redes hasta el destino, cuya dirección vendrá indicada en la dirección del nivel de red destino de la PDU.

La utilización de identificadores de la conexión tiene ventajas una de ellas y muy importante es el **encaminamiento** el cual al establecer una conexión se debe definir una ruta fija. El identificador de la conexión sirve para que los sistemas intermedios (por ejemplo, los nodos de conmutación de paquetes) identifiquen la ruta y puedan encaminar las PDU futuras.

Multiplexaje: El multiplexaje es un concepto relacionado con el direccionamiento. Un posible esquema de multiplexaje es aquel en el que se establecen varias conexiones dentro de un único sistema. La multiplexación también puede llevar a cabo usando los nombres de los puertos, los cuales a su vez son múltiples conexiones.

Servicios de Transmisión: Servicios a través de los cuales se permite enviar y recibir información simultáneamente. Existen servicios adicionales que se proporcionan a las entidades que lo utilicen como: Prioridad, Calidad de servicio y Seguridad.

1.2.3.- Arquitecturas

Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares el Protocolo de Control de Transmisión (TCP/IP, por sus siglas en inglés, Transmission Control Protocol / Internet Protocol) y el modelo de Interconexión de Sistemas Abiertos (OSI, por sus siglas en inglés, Open System Interconnection). TCP/IP es la arquitectura más adoptada para la **interconexión de sistemas,** mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación.

La idea de una arquitectura de protocolos para la transferencia de información nace con la idea de hacer que dos o más equipos tengan una conectividad, siguiendo una serie de pasos que están conformados en capas y que cuentan con protocolos que les ayudan a cumplir ciertas tareas, hoy en día se cuenta con varias arquitecturas que ayudan a establecer una comunicación, en el siguiente tema se hablara de cómo se constituyen estas dos arquitecturas las cuales son muy importantes para el proyecto.

1.3.- Modelo de Referencia OSI y Pila TCP/IP

TCP/IP reconoce que la tarea de la comunicación es lo suficientemente compleja y diversa como para realizarla en una única unidad. Consecuentemente, la tarea se descompone en diversos módulos (capas), que se pueden comunicar con sus módulos pares del sistema remoto.

Una capa dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras capas. Las reglas de diseño del programa de calidad dictan que estas capas se deben agrupar en una forma modular y jerárquica.

El modelo OSI se basa en el mismo razonamiento, pero introduce un paso más. El siguiente paso en el modelo OSI está en reconocer que, en muchos aspectos, los protocolos en el mismo nivel de la jerarquía tienen algunas características comunes. Esto desemboca ineludiblemente en el concepto de nivel o capa, así como en el intento de describir de una forma abstracta las características comunes de los protocolos en un nivel dado.

1.3.1.-Arquitectura TCP/IP

A continuación se describe la arquitectura TCP/IP la cual es desarrollada en el año de 1973 por el informático estadounidense Vinton Cerf debido a su investigación y desarrollo llevando a cabo una red experimental de conmutación de paquetes la Agencia de Proyectos de Investigación de Red (ARPANET, por sus siglas en inglés, Advanced Research Projects Agency Network), financiada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA, por sus siglas en inglés, Defense Advanced Research Projects Agency), y se denomina mundialmente como la familia de protocolos TCP/IP. Esta familia llena de protocolos que se han establecido como los estándares de Internet

La pila TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos que permiten que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser direccionados, transmitidos, enrutados y recibidos por el destinatario.

Cuando se emplea TCP/IP, la información viaja entre emisor y receptor en segmentos creados por TCP y encapsulados en paquetes por IP, los paquetes son llamados Datagramas IP.

TCP/IP ofrece ventajas significativas sobre otros protocolos de red. Una de tales ventajas es que trabaja sobre una gran variedad de componentes físicos y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este modelo, recordando que una red heterogénea es una red de conexión de computadoras y otros dispositivos con diferentes sistemas operativos y/o protocolos.

La pila TCP/IP está estructurada en cinco niveles, cada uno encargado de una faceta diferente de la comunicación: el nivel de red, el nivel de Internet, el nivel de transporte, y el nivel de aplicación, como se puede observar en la Figura 1.4.

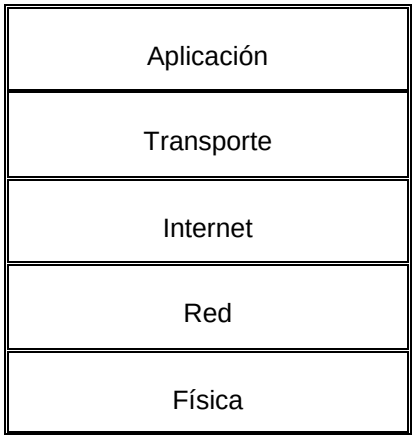


Figura 1.4 Modelo TCP/IP

La **capa física** define la interfaz física entre el dispositivo de transmisión de datos (por ejemplo, una computadora) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos, y cuestiones similares.

La **capa de acceso a la red** es responsable del intercambio de datos entre el sistema final y la red a la cual se está conectado. El emisor debe proporcionar a la red la dirección del destino, de tal manera que la red pueda encaminar los datos hasta el destino apropiados. El programa en particular que se usa en esta capa dependerá del tipo de red que se disponga; se han desarrollado diversos estándares para conmutación de circuitos, conmutación de paquetes, redes de área local (Ethernet), entre otros.

Otros protocolos especializados en esta capa son:

Unidad Máxima de Transferencia (MTU, por sus siglas en inglés, Maxim Transfer Unit): Determina el tamaño máximo de cada paquete en cualquier transmisión.

Protocolo de Resolución de Direcciones (ARP, por sus siglas en inglés, Address Resolution Protocol): Permite que se conozca la dirección física de una tarjeta de interfaz de red o mejor conocida como dirección MAC la cual se asigna en la fábrica y es un numero de 48 bits y es único e irrepetible pero esta dirección no permite conectarse a Internet, sino que utiliza una dirección lógica asignada por un organismo: la dirección IP la cual permite navegar en Internet.

Protocolo de Resolución Inversa de Direcciones (RARP, por sus siglas en inglés, Reverse Address Resolution Protocol): Este protocolo no es tan utilizado. Es un tipo de directorio inverso de direcciones lógicas y físicas. En realidad, el protocolo RARP se usa esencialmente para las estaciones de trabajo sin discos duros que desean conocer su dirección física.

En situaciones en las que los dos dispositivos estén conectados a redes diferentes, se necesitará una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. Esta es la función de la **capa de Internet.** El protocolo de internet (IP). Transportara los bloques de datos desde una computadora hasta otra, a través de uno o varios dispositivos de encaminamiento.

Este protocolo se implementa tanto en los sistemas finales como en los enrutadores intermedios. Un enrutador es un dispositivo con capacidad de procesamiento que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar el destino.

Lo protocolo más importantes dentro de esta capa son: IP, Protocolo de Control de Mensajes de Internet (ICMP, por sus siglas en inglés, Internet Control Message Protocol) y el Protocolo de Administración de Grupos de Internet (IGMP, por sus siglas en inglés, Internet Group Message Protocol).

ICMP: Es el sub protocolo de control y notificación de errores del Protocolo de Internet. Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un enrutador o un dispositivo no puede ser localizado.

IGMP: Es un protocolo de Internet que proporciona una forma para un ordenador con Internet, informar su pertenencia al grupo de multidifusión a enrutadores adyacentes. La multidifusión permite a una computadora en Internet enviar contenido a varios equipos que se han identificado como interesado en recibir el contenido originario de computadoras.

Los procedimientos que garantizan una transmisión segura están localizados en la **capa de transporte**. El protocolo TCP es el más utilizado para proporcionar está funcionalidad.

La capa de transporte no se preocupa de la ruta que van a seguir los datos para llegar a su destino final. Simplemente considera que la comunicación entre ambos extremos está ya establecida y la utiliza. Los dos protocolos principales de la capa de transporte de la pila TCP/IP son: TCP y el Protocolo de Datagramas de Usuario (UDP, por sus siglas en inglés, User Datagram Protocol).

TCP: Se implementa en los sistemas finales; guarda un registro de bloques de datos para asegurar que todos se entregan de forma segura a la aplicación apropiada.

Algunas de sus características son:

- TCP permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- TCP permite el monitoreo del flujo de los datos y así evitar la saturación de la red.
- TCP permite que los datos se formen en segmentos de longitud variable para "entregarlos" al protocolo IP.
- TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- Por último, TCP permite comenzar y finalizar la comunicación amablemente.

Es importante saber que TCP es conocido como un protocolo orientado a la conexión, lo que significa que una conexión es establecida y mantenida hasta el momento en que se han intercambiado el mensaje o mensajes para ser canjeado por los programas de aplicación en cada extremo.

UDP: Por el contrario UDP es sencillo pues es un protocolo no orientado a conexión, es una alternativa para el Protocolo de Control de transmisión (TCP) solo que ofrece una cantidad limitada de servicio cuando se intercambian mensajes entre ordenadores en una red que utiliza el protocolo de Internet. UDP no proporciona el servicio de dividir un mensaje en paquetes (datagramas) y lo vuelva a reensamblar en el otro extremo, UDP debe ser capaz de asegurarse de que todo el mensaje ha llegado y está en el orden correcto.

La gran diferencia entre estos protocolos es su orientación a la conexión pues mientras que en TCP siempre se mantiene una conexión en UDP, no es necesario establecerla, hablando de los paquetes enviados en TCP se tiene una buena recepción de ellos pues se encarga de que hayan llegado bien y sin alterarse. En el caso de UDP también se encarga de que los paquetes lleguen bien pero no es capaz de verificar si estos llegaron a su destino y de manera correcta.

Por último la **capa de aplicación** contiene la lógica necesaria para posibilitar las distintas aplicaciones de usuario. Dicha capa corresponde con los programas de usuario que llama a los servicios de aplicación TCP/IP, dentro de los cuales están: HTTP, TELNET, FTP, SMTP, SNMP, etc.

Protocolo de Transferencia de Hipertexto (HTTP, por sus siglas en inglés, Hypertext Transfer Protocol): Es uno de los protocolos más recientes. Se utiliza para manejar la consulta de hipertexto y el acceso de datos con Red Informática Mundial (WWW,

por sus siglas en inglés, World Wide Web). El protocolo HTTP funciona a través de solicitudes y respuestas entre un cliente (por ejemplo un navegador de Internet) y un servidor (por ejemplo la computadora donde residen páginas web). A una secuencia de estas solicitudes se le conoce como sesión de HTTP.

TELNET: Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (computadora) con un intérprete de instrucciones (del lado del servidor). El protocolo Telnet se aplica en una conexión TCP para enviar datos en el formato del Código de Intercambio de Información (ASCII, por sus silgas en inglés, American Standard Code for Information Interchange) codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet.

Protocolo de Transferencia de Archivos (FTP, por sus siglas en inglés, File Transfer Protocol): Es un protocolo para transferir archivos, el objetivo del protocolo FTP es:

- Permitir que equipos remotos puedan compartir archivos
- Permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- Permitir una transferencia de datos eficaz

Protocolo Simple de Transferencia de Correo (SMTP, por sus siglas en inglés, Simple Mail Transfer Protocol): Es el protocolo estándar que permite la transferencia de correo electrónico de un servidor a otro mediante una conexión punto a punto. Éste es un protocolo que funciona en línea, encapsulado en una trama TCP/IP.

Protocolo Simple de Administración de Red (SNMP, por sus siglas en inglés, Simple Network Management Protocol): Es un protocolo que les permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red.

Algunos otros protocolos más especializados son el Protocolo de Configuración Dinámica de Host (DHCP, por sus siglas en inglés, Dynamic Host Configuration Protocol) y Sistema de Nombres de Dominio (DNS, por sus siglas en inglés, Domain Name System)

DHCP: Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente.

DNS: Cada equipo conectado directamente a Internet tiene al menos una dirección IP específica. Sin embargo, los usuarios no desean trabajar con direcciones numéricas, como por ejemplo 194.153.205.26, sino con un nombre de dominio o más específicamente, con direcciones (llamadas direcciones FQDN) como por ejemplo “www.ipn.com.mx”.

TCP/IP es creado con la finalidad de resolver problemas entre redes heterogéneas o dicho de otra forma entre tecnologías diferentes entre sí.

1.3.2.- Modelo OSI

El modelo OSI se desarrolló por la Organización Internacional de Estandarización (ISO, por sus siglas en inglés, International Organization for Standarization) como una arquitectura para comunicaciones entre computadores, con el objetivo de ser el marco de referencia en el desarrollo de protocolos estándares. OSI considera siete capas:

- Aplicación
- Presentación
- Sesión
- Transporte
- Red
- Enlace de Datos
- Física

Cada capa realiza un conjunto de funciones relacionadas entre sí, necesarias para comunicarse con otros sistemas. Cada capa se sustenta en la capa inmediatamente inferior, la cual realizará funciones más primitivas, ocultando los detalles de las capas superiores. Una capa proporciona servicios a la capa inmediatamente superior.

En la figura 1.5 muestra las capas del modelo OSI. La intención del modelo OSI es que los protocolos se desarrollen de forma tal que realicen las funciones de cada una de las capas.

Figura 1.5 Las capas del Modelo OSI

A continuación se explicara cada una de las capas del Modelo OSI:

Capa 7 Aplicación: Esta capa trabaja con el programa de aplicación para proporcionar funciones de comunicaciones según sea necesario. También funciona con aplicaciones como DNS, FTP, HTTP, SMTP, TELNET y emulación de terminal.

Capa 6 Presentación: Esta capa comprueba los datos para asegurar que sea compatible con los recursos de comunicaciones. Asegura la compatibilidad entre los formatos de datos a nivel de las aplicaciones y los niveles inferiores. También maneja los datos necesarios de conversión de formato o código, así como compresión de datos y cifrado.

Capa 5 Sesión: Maneja las funciones de autenticación y autorización. También gestiona la conexión entre los dos dispositivos de comunicación, establecer una conexión, manteniendo la conexión y la terminación en última instancia. Esta capa verifica que los datos se entregan correctamente.

Capa 4 Transporte: Esta capa proporciona seguridad, transferencia transparente de datos entre los puntos finales; proporciona además procedimientos de recuperación de errores y control de flujo origen-destino.

Capa 3 Red: La capa de red se encarga del encaminamiento de paquetes mediante direccionamiento lógico y funciones de conmutación, también es responsable del establecimiento, mantenimiento y cierre de conexiones.

Capa 2 Enlace de Datos: Proporciona un servicio de transferencia de datos seguro a través del enlace físico; envía bloques de datos (tramas) llevando a cabo la sincronización, el control de errores y de flujo necesarios.

Capa 1 Física: Define la conexión física entre el nodo y la red, incluyendo los aspectos físicos, mecánicos y aspectos eléctricos, su unidad de transmisión es el bit.

En la figura 1.6 se hace una representación de la funcionalidad del modelo OSI

Figura 1.6 Los flujos de datos viajan hacia abajo sobre la capa de tránsito, sobre el enlace físico, y luego hacía arriba sobre la capa de recibimiento.

Los diseñadores del modelo OSI consideraron que este modelo y los protocolos asociados llegarían a dominar las comunicaciones entre computadoras, reemplazando eventualmente las implementaciones particulares de protocolos, así como a modelos rivales tales como TCP/IP. Sin embargo, esto no ha sido así. Aunque se han desarrollado muchos protocolos de utilidad dentro del contexto del modelo OSI, el modelo de las siete capas en su conjunto no ha prosperado. Por el contrario, la arquitectura TCP/IP se ha hecho dominante.

Por tal motivo se hablara sobre una comparación del Modelo OSI contra la arquitectura TCP/IP.

1.3.3.- Comparativa

La Figura 1.7 muestra las capas de las arquitecturas TCP/IP y OSI, indicando la posible correspondencia en términos de funcionalidad entre ambas.

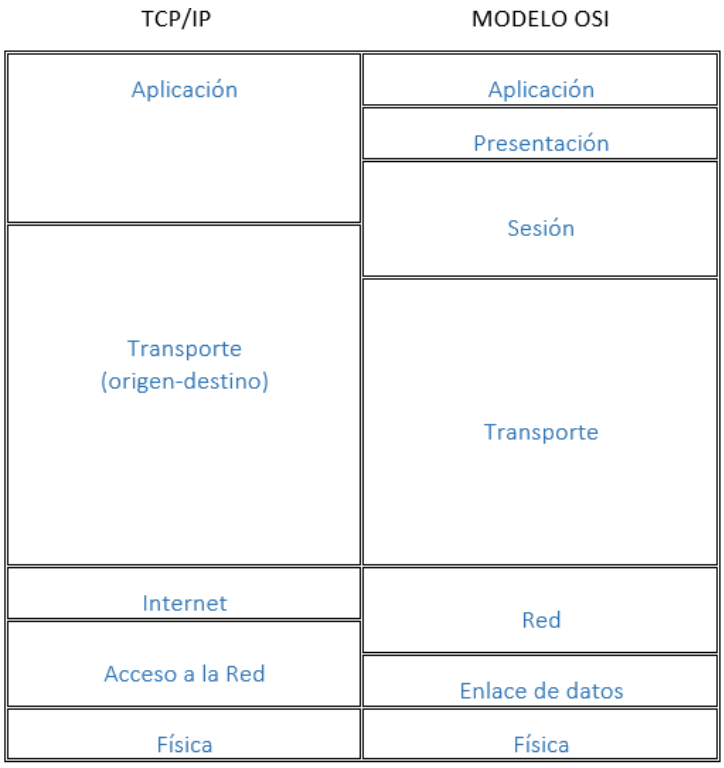


Figura 1.7 Comparación de la arquitectura TCP/IP contra el Modelo OSI

El modelo de referencia OSI y la arquitectura TCP/IP tienen mucho en común. Los dos se basan en el concepto de una pila de protocolos independientes. También la funcionalidad de las capas es muy similar. Por ejemplo, en ambos las capas por encima de la de transporte, incluida ésta, están ahí para prestar un servicio de transporte de extremo a extremo, independiente de la red, a los procesos que deseen comunicarse. Estas capas forman el proveedor de transporte. También en ambos modelos, las capas encima de la de transporte son usuarios del servicio de transporte orientados a aplicaciones.

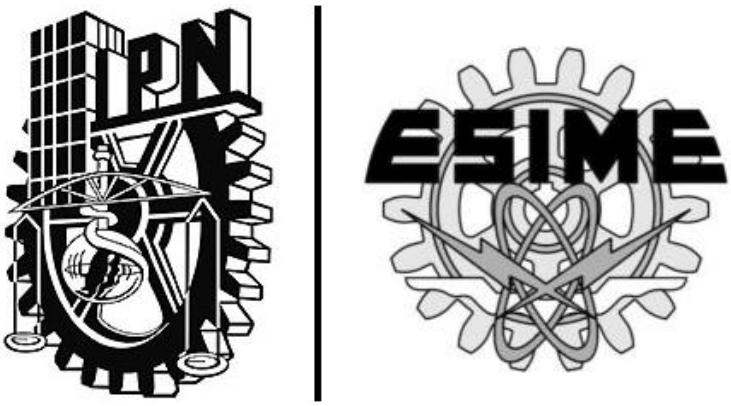
A pesar de estas similitudes fundamentales, las dos arquitecturas tienen también muchas diferencias. Las diferencias entre la arquitectura OSI y la del TCP/IP se relacionan con las capas encima del nivel de transporte y aquellas del nivel de red. OSI tiene una capa de sesión y una de presentación en tanto que TCP/IP combina

ambas en una capa de aplicación. El requerimiento de un protocolo sin conexión, también requirió que el TCP/IP incluyera además, las capas de sesión y presentación del modelo OSI en la capa de aplicación de TCP/IP.

Originalmente, la arquitectura TCP/IP no distinguía entre servicio, interfaz y protocolo, aunque las personas han tratado de readaptar con el propósito de hacerlo más parecido a OSI. Como consecuencia, los protocolos del modelo OSI están mejor ocultos que los del modelo TCP/IP y se pueden reemplazar fácilmente conforme cambia la tecnología. La facilidad para remplazar tales cambios es uno de los objetivos principales de tener protocolos en capas.

El modelo de referencia OSI se vislumbró antes de que se inventaran los protocolos correspondientes. Esta clasificación significa que el modelo no estaba diseñado para un conjunto particular de protocolos, un hecho que lo hizo general. Una deficiencia de esta clasificación es que los diseñadores no tenían una idea concreta de que funcionalidad poner en qué capa.

Con TCP/IP sucedió lo contrario; los protocolos llegaron primero y el modelo fue en realidad una descripción de los protocolos existentes. No había problemas para ajustar los protocolos al modelo. El único problema era que el modelo no aceptaba otras pilas de protocolos. Como consecuencia no era útil para describir otras redes que no fueran TCP/IP.



CAPÍTULO 2 | "Protocolos de Internet IPv4 e IPv6

Capítulo 2: Protocolos de Internet IPv4 e IPv6

El presente capítulo se basa en los servicios estandarizados llamados Protocolos de Internet versiones 4 y 6, se presentarán también el esquema de direccionamiento usado por IP y se explicará la división de las clases de direcciones del IP. Por otro lado, se definirá cada parte de la cabecera de ambos protocolos y su comparación.

2.1 Características principales de IPv4

A través de los últimos años el internet o red mundial ha evolucionado, en muchos aspectos como el aumento de usuarios, multimedia y ancho de banda., siendo así una red más interactiva entre los usuarios que la accedan, pero esto ha tenido consecuencia en la actual estructura de la red. Entre los problemas actuales esta la limitación o escases de direcciones públicas, aumento en las tablas de enrutamiento, la necesidad de soportar Calidad de Servicio (QoS, por sus siglas en inglés, Quality of Service) y seguridad a nivel de red, lo que ha provocado la evolución del protocolo actualmente que es llamado IPv4.

El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por conmutación de paquetes. El protocolo de internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas, unidades principales de información de Internet, desde el origen al destino, donde origen y destino son computadoras, identificadas por direcciones de longitud fija. El protocolo de internet también se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

Las principales características del protocolo IPv4 son:

- **Enrutamiento y direccionamiento.-** Proporciona únicamente una dirección a cada uno de los dispositivos de redes de paquetes. Es decir, que IPv4 principalmente diseñado para proveer el enrutamiento de información (paquetes) mediante redes de diversa complejidad.

- **Encapsulación.-** Es una división antigua de TCP/IP, localizado en la capa 3 del modelo ISO/OSI y funciona sobre diversos protocolos de nivel inferior.

- **Mejor esfuerzo:** El protocolo IP provee un servicio de transmisión de paquetes no fiable (o de mejor esfuerzo). No se asegura que los paquetes enviados lleguen correctamente al destino.

2.1.1 Clases de direcciones

Las direcciones en IPv4 tienen una longitud de 32 bits, las direcciones son de una longitud fija de 4 octetos, dicha longitud está representada por 4 clases (A, B, C y D) que están representadas por un número decimal en el intervalo de 0 a 255, es decir, el rango se escribe desde 0.0.0.0 a 255.255.255.255, lo que es una limitante en la actualidad ya que existen combinaciones del tipo $2^{32} = 4\,294\,967\,296$ o sea 4 billones de direcciones.

Las clases A, B, C han sido divididas en partes fijas, dichas divisiones son muy conocidas en el rango ya mencionado anteriormente. Adicionalmente, existen direcciones del tipo D y E reservadas para procesos experimentales y multicast, es decir para comunicaciones multipunto. La figura 2.1 ilustra la identificación de las clases de direcciones IP.

Clase/bits	0	1 7	16 24 31
Clase A	0	Red	Número de usuario o host
Clase B	10	Número de Red	Número de usuario o host
Clase C	110	Número de Red	Numero de usuario
Clase D	1110	Direccion de Multicast	
Clase E	1111	Reservado	

Figura 2.1 Identificación de las clases de direcciones IP

De acuerdo a la Figura 2.1 en la cual se muestran cinco clases de direcciones; los bits de la izquierda identifican las clases y la división el prefijo y el sufijo, siguiendo la convención de los protocolos TCP/IP, se debe de numerar los bits de izquierda a derecha y de numerar como cero el primer bit. Las clases A, B y C se denominan clases primarias, porque emplean direcciones de computadoras. La clase D se utiliza para comunicación multipunto, estas permiten realizar transmisiones a un grupo de usuarios o de computadoras. Cuando se envía un paquete IP a una dirección multicast, este será recibido por todas las computadoras que conforman dicho grupo. El primer byte de estas direcciones puede tomar un valor comprendido entre 224 y 239.

Cada dirección de red tiene un rango específico el cual se muestra en la tabla 2.1.

Clase	Rango de dirección
A	0.0.0.0 a 127.255.255.255
B	128.0.0.0 a 191.255.255.255
C	192.0.0.0 a 223.255.255.255
D	224.0.0.0 a 239.255.255.255
E	240.0.0.0 a 255.255.255.255

Tabla 2.1 Rango de dirección

- Las direcciones de clase A están concebidas para las redes compuestas de numerosas computadoras. Se usa el primer bit del espacio de los 32 bits (bit 0) para identificar a la clase A; este bit se pone en 0. Los bits del 1 al 7 representan la identificación de la red y los bits del 8 al 31 identifican a la computadora personal, dispositivo terminal en la red.

  Por convención, el uso de todos los bits en “1” o en “0” está prohibido tanto para el campo de red como para el campo de las computadoras, por lo tanto se le restan 2 bits (red y broadcast).

- En la clase B las direcciones se emplean en redes constituidas por un número medio de ordenadores. Se permiten hasta $2^{14} - 2$, es decir, 16 382 redes y $2^{16} - 2 = 65\,134$ dispositivos para cada red. La clase B usa los primeros 2 bits (bit 0 y bit 1) para la identificación de esta clase en el campo de los 32 bits. Estos bits son puestos en 1 y 0 respectivamente. Los bits del 2 al 15 representan la ID de la red mientras que los bits del 16 al 31 identifican a la computadora personal.
- La clase C, las direcciones se destinan a redes con pocos ordenadores o dispositivos. Usa los primeros 3 bits (bit 0, bit 1 y bit 2) para la identificación de esta clase en el campo de los 32 bits. Estos bits son puestos en 1, 1 y 0 respectivamente. Los bits del 3 al 23 representan la ID de la red mientras que los bits del 24 al 31 identifican a la computadora personal. Esta clase soporta cerca de 2 millones de redes $(2^{21} - 2)$ y $2^8 - 2 = 254$ dispositivos para cada red.

- La clase D usa los primeros 4 bits (bit 0, bit 1, bit 2 y bit 3) para la identificación de esta clase en el campo de los 32 bits. Estos bits son puestos en 1, 1, 1 y 0 respectivamente. Este tipo de clase se usa para multicast, en el que todos los dispositivos de la red reciben el mismo paquete. Esto se usa en aplicaciones de IP multicast por ejemplo Televisión por Protocolo de Internet (IPTV, por sus siglas en inglés, Internet Protocol Television).

- Las direcciones privadas están en los rangos de 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16. En el caso de direcciones privadas, una función Traducción de Dirección de Red (NAT, por sus siglas en inglés, Network Address Translation) se emplea para asignar la dirección interna a una dirección externa pública cuando se cruza la frontera de la red privada a la pública.

Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255 o 127.0.0.0/8 en la notación Enrutamientos entre Dominios sin Clases (CIDR, por sus siglas en inglés, Classless Inter-Domain Routing), está reservado para la comunicación de la computadora local. Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada y cualquier paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

Por lo tanto, existen bloques de direcciones que están reservados y se muestran la tabla 2.2:

Bloque de direcciones CIDR	Descripción	Referencia
0.0.0.0/8	Red actual (solo valido como dirección de origen)	RFC 1700
10.0.0.0/8	Red Privada	RFC 1918
127.0.0.0/8	Computadora local	RFC 1700
128.0.0.0/16	Reservado	
169.254.0.0/16	Red Privada (Zeroconfig)	RFC 3927
172.16.0.0/12	Red Privada	RFC 1918
192.168.0.0/16	Red Privada	RFC 1918
255.255.255.255	Broadcast	

Tabla 2.2 Direcciones Privadas

2.1.2 Cabecera del Protocolo IPv4

El protocolo de Internet IP, es la parte fundamental sustentada por el sistema TCP/IP y de todo el funcionamiento de Internet. La unidad de datos del IP es el datagrama cuya cabecera se muestra en la figura 2.2.

<table>
<tr><td>Versión (4 bits)</td><td>IHL (4 bits)</td><td>Tipo de servicio (8 bits)</td><td colspan="2">Longitud total (16 bits)</td></tr>
<tr><td colspan="3">Identificación (16 bits)</td><td>Bandera (3bits)</td><td>Fragmentación (13bits)</td></tr>
<tr><td colspan="2">TTL (8 bits)</td><td>Protocolo (8 bits)</td><td colspan="2">Comprobación (16 bits)</td></tr>
<tr><td colspan="5">Dirección fuente (32 bits)</td></tr>
<tr><td colspan="5">Dirección destino (32 bits)</td></tr>
</table>

Figura 2.2. Cabecera de IPv4

En la figura 2.2 se ilustra a un datagrama IP, cuya estructura es en bloques de 32 bits (4 bytes), su transmisión consiste en enviar primero el bit 0, luego el bit 1, 2,3… y así sucesivamente hasta finalizar el datagrama. Dicho orden se denomina “orden de bytes de red” (“network byte order”), él mismo es muy importante, debido a que las diferentes computadoras tienen diversos sistemas de almacenamiento de bits en memoria.

Según el modelo TCP/IP el protocolo de capa 3 permite direccionar los datagramas en la capa de red, este encabezado se superpone al datagrama manejado, es decir, las características de ruteo y transmisión. En la capa inmediatamente inferior a TCP se agrega el encabezado, quedando el datagrama tal y como se muestra en la figura 2.3.

<table>
<tr><td>Encabezado IP
(20 bytes)</td><td>Encabezado TCP
(20 bytes)</td><td>Datos</td></tr>
</table>

Figura 2.3. Configuración de un datagrama IPv4

La longitud que tiene el encabezado IP en la capa de red es de 170 bits, que aproximadamente es 20 bytes, formada por diversos campos con distintos significados como se observa en la figura 2.2. Los campos descritos en la figura 2.2 se definen a continuación.

- **Versión:** Indica el número de la versión del Protocolo de Internet, es decir, que para IPv4 será 4.

- **Longitud de encabezado:** Describe la longitud del encabezado en número de grupos de 32 bits cada uno de 4 bits.

- **Tipo de servicio:** Permite saber la importancia de los datos enviados, condicionando la forma en que serán tratados en la transmisión de 8 bits.

- **Longitud total:** Indica la longitud completa en bytes del datagrama de 16 bits, incluyendo el encabezado y los datos. En la práctica el datagrama es pequeño (16 bits) y teóricamente no será mayor a 65,535 bytes.

- **Identificación:** Utilizada para el ensamble de los fragmentos de un datagrama de 16 bits.
- **Banderas:** Es un indicador empleado en la fragmentación de 3 bits.

- **Fragmentación:** Permite ensamblar los datagramas previamente fragmentados, cuyo valor es de 64 bits (grupos de 8 bytes), el primer grupo de una serie de fragmentos contendrá en este campo el valor 0.

- **Límite de existencia (TTL, por sus siglas en inglés, Time To Live):** Es un número que disminuye cada vez que el paquete de datos (8 bits) pasa por un nodo de red, si el valor toma un 0 indica que el paquete se ha descartado. Por cuestiones de seguridad se debe evadir la verificación de redundancia cíclica, empleado por razones de seguridad o confiabilidad siendo poco probable que esto ocurra en una red bien diseñada.

- **Protocolo:** Es un número que se emplea para definir el protocolo perteneciente al datagrama (8 bits), de tal manera que sea tratado eficientemente cuando llegue a su destino.

- **Comprobación:** Permite verificar que los datos que contiene el encabezado de IP sean correctos, dicha eficiencia no se utiliza para evaluar los datos ya incluidos, sino que los datos de usuario se comprueban posteriormente del encabezado siguiente, correspondiente al nivel de capa de transporte (16 bits). Adicionalmente, si se cambia la opción de encabezado, dicho campo será calculado nuevamente.

- **Dirección fuente:** Es aquella que contiene la dirección del usuario en la que envía el paquete de datos de 32 bits.

- **Dirección destino:** Es aquella dirección del usuario que recibe la información, es decir, los enrutadores o compuerta de enlace, conocen la dirección para hacer llegar correctamente el paquete de datos de 32 bits.

- Después del campo dirección destino, existe un par de campos llamados opciones y valor de relleno; el campo opciones puede o no aparecer en los datagramas. Deben ser implementados por todos los módulos IP. Lo que es opcional es su transmisión en cualquier datagrama en particular, no su implementación. Mientras que el campo Valor de relleno se usa para asegurar que la cabecera internet ocupa un múltiplo de 32 bits. El valor de relleno es cero.

2.2 Restricciones del protocolo IPv4

La versión de IPv4 usada actualmente en Internet no ha cambiado sustancialmente desde su publicación inicial en 1981. IPv4 ha demostrado ser un protocolo robusto, fácil de implementar y con la capacidad de operar sobre diversos protocolos de capa 2. Si bien fue diseñado inicialmente para interconectar unos pocos computadores en redes simples, ha sido capaz de soportar el explosivo crecimiento de internet.

2.2.1 Problemática principal en IPv4

En aquel momento tanto el número de ordenadores conectados como las expectativas de crecimiento eran mucho más moderados de lo que han sido realmente, y por tanto la suposición de que un tamaño de 32 bits sería suficiente parecía razonable. De esta manera, se puede justificar la revisión de la versión 4 del protocolo IP desde dos puntos de vista principalmente:

- **Técnico**.- Donde el direccionamiento es insuficiente, debido a la gran demanda y que a futuro incrementa considerablemente. Las tablas de enrutamiento o de direcciones, son las encargadas de almacenar los enrutadores internamente, y empleados para saber hacia dónde deben

enrutar un datagrama, son excesivamente grandes debido a la enorme cantidad de direcciones que existen actualmente y al sistema de encaminamiento utilizado, lo que obligaría a los enrutadores a mantener grandes cantidades de direcciones para conocer hacia dónde deben redireccionar los datagramas.

- **Social:** Las necesidades de los usuarios de Internet han aumentado espectacularmente, exigiendo nuevas capacidades (seguridad, privacidad, comercio electrónico, velocidad, etc.) que la versión 4 no puede proporcionar.

2.2.2 Esfuerzos de conservación en IPv4

Debido a las problemáticas e inconvenientes que se presentan en IPv4 se han propuesto o desarrollado métodos para reducir dichos problemas relacionados con el direccionamiento IPv4. Las soluciones más importantes son:

- RFC 917 – Subredes de Internet *(*Internet Subnets*,* 1984) y RFC 950 – Procedimiento Estándar de Subredes de Internet (*Internet Standard* Subnetting Procedure, 1985). Introducen el **«subnetting»**, basado en la necesidad de contar con un tercer nivel de jerarquía.

- **VLSM**. El RFC 1009 implementado en 1987, indica el uso de subredes con prefijos de diferentes tamaños.

- A principios de los 90 se implementa **CIDR**, cuyas especificaciones fueron liberados en los RFCs 1517, 1518, 1519 y 1520. Elimina el uso de las clases y permite la agregación de rutas.

- **NAT.** Especificado originalmente en el RFC 1631. Un método particular de translación conocido como PAT (Traducción de Direcciones de Puertos), la cual permite un ahorro de IP`s ya que pueden salir innumerables direcciones privadas, asignándoles a cada salida el mismo IP, pero con diferente número de puerto, lo que permite ahorrar el uso de direcciones IP.

- **PPP/DHCP.** Asignación dinámica de direcciones IP.

Todo esto lleva al agotamiento de direcciones IP, la cual implica que exista otro método para ofrecer un mayor número de direcciones y que estas no se agoten.

2.3 Protocolo de Internet versión 6

En la década de los 90 se empezó a observar un crecimiento considerable de usuarios de internet y por lo tanto las direcciones de IPv4 de 32 bits se estaban agotando, por lo que el Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés, Internet Engineering Task Force) empezó a trabajar en el desarrollo de una nueva versión de IP además de que vieron la oportunidad de ajustar y aumentar otros aspectos de IPv4.

En Julio de 1992 la IETF hizo una convocatoria solicitando las mejores propuestas para una nueva generación del IP. Se recibieron varias propuestas y en 1994 surgió el diseño final y a la que se denominaría como IP siguiente generación (IPng, por sus siglas en inglés, Internet Protocol Next Generation) RFC 1752. Esta nueva versión de IP nunca tendría problema alguno con la escasez de direcciones ya que se incrementaría su tamaño a 128 bits, sería una versión mucho más flexible y eficiente, y a la que finalmente se le dio el nombre de IPv6.

El protocolo de internet versión 6 está definido por el RFC 2460, es la nueva versión del Protocolo Internet diseñado como el sucesor para IP versión 4 definido en el RFC 791 y que actualmente está implementado en la mayoría de los dispositivos que acceden a internet, el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

2.3.1 Características principales de IPv6

El protocolo IPv6 conserva muchas de las características de IPv4, sus diseñadores han caracterizado a IPv6 como si fuera básicamente el mismo que IPv4 solo que con unas cuantas modificaciones. Un ejemplo de ello es que IPv6 soporta la entrega sin conexión, es decir permite que cada datagrama sea enrutado independientemente, o dicho de otra forma permite al emisor seleccionar el tamaño de un datagrama y requiere que el emisor especifique el número máximo de saltos que un datagrama puede realizar antes de ser eliminado.

También conserva gran parte de los conceptos proporcionados por IPv4, incluyendo capacidad de fragmentación y ruteo de fuente.

Pero a pesar de tener algunas similitudes, IPv6 cambia algunos detalles, como por ejemplo, en IPv6 se utilizan direcciones largas y agrega unas cuantas características nuevas, cabe mencionar algo muy importante, en IPv6 revisa completamente el formato de los datagramas, ya que es reemplazada la opción de longitud variable de IPv4 por una serie de encabezados fijos. Más adelante se examinarán los detalles después de considerar los cambios más significativos.

Los cambios introducidos para IPv6 pueden agruparse en cinco categorías:

- Direcciones de mayor longitud: El nuevo tamaño de las direcciones es el cambio más notable. El IPv6 cuadruplica el tamaño de las direcciones de IPv4, va de 32 bits a 128 bits. Es tan grande que no podrá agotarse en un futuro.

- Un mecanismo de opciones mejorado: Las opciones de IPv6 se encuentran en cabeceras opcionales separadas situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6 en comparación a los datagramas IPv4. Eso también hace que sea más fácil incorporar opciones adicionales.

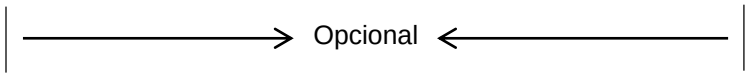
- Direcciones de autoconfiguración: Esta capacidad proporciona una asignación dinámica de direcciones IPv6.

- Aumento de la flexibilidad en el direccionamiento: IPv6 incluye el concepto de una dirección anycast, mediante la cual un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos. Se mejora la escalabilidad del encaminamiento multicast con la incorporación de un campo de acción a las direcciones multicast.

- Facilidad para la asignación de recursos: En lugar del campo tipo-de-servicio de IPv4, IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial. Esto ayuda al tratamiento del tráfico especializado como el de video en tiempo real.

2.3.2 Formato general de un datagrama IPv6

IPv6 cambia completamente el formato de datagrama. Como se muestra en la figura 2.4, un datagrama IPv6, tiene un encabezado base de tamaño fijo, seguidos por ceros o más encabezados de extensión, seguidos a su vez por datos.



Encabezado Base	Extensión 1 de encabezado	…	Encabezado N de encabezado	Datos

Figura 2.4 Formato general de un datagrama IPv6 con varios encabezados. Sólo el encabezado base es indispensable, los encabezados de extensión son opcionales.

2.4 Formato de la cabecera IPv6

La cabecera de IPv6, descrita en el RFC 2460, elimina o hace opcionales varios campos de la cabecera de IPv4, consiguiendo una cabecera de tamaño fijo y más simple, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el coste en ancho de banda de la cabecera de IPv6. La cabecera básica de IPv6 tiene una longitud fija de 40 octetos.

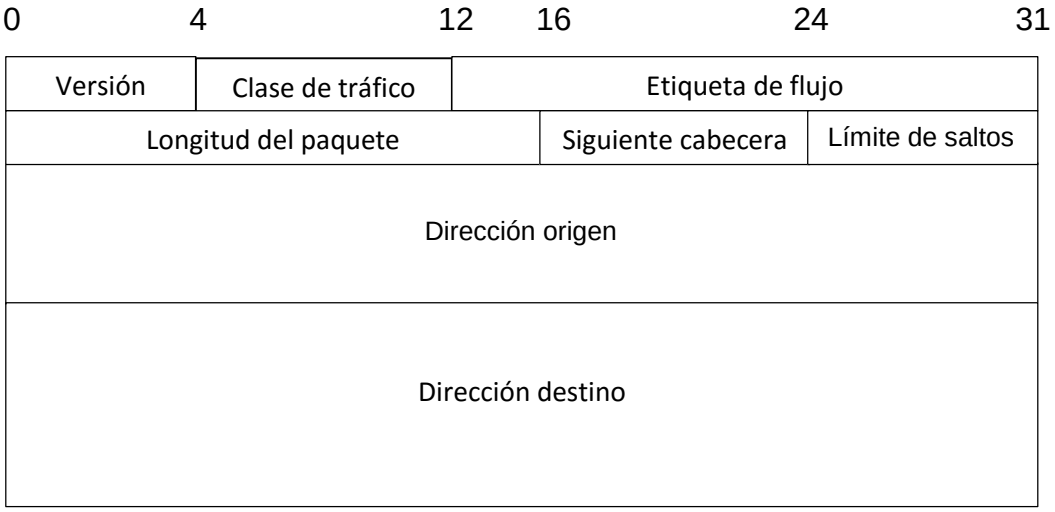


Figura 2.5 Formato de la cabecera base de IPv6.

2.4.1 Descripción de los campos de la cabecera de IPv6

- **Versión (4 bits):** Es el número de versión de IP, es decir, 6.

- **Clase de tráfico (8 bits):** El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y del 8-15 para tráfico de video y audio sin control de la congestión.

- **Etiqueta de flujo (20 bits):** El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen especifico a un destino específico. Un flujo es identificado únicamente por la combinación de una dirección fuente y una etiqueta de 20 bits. De esta manera, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo.

- **Longitud del paquete (16 bits):** Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.

- **Siguiente cabecera (8 bits):** Indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP (Protocolo de Datagrama de Usuario), ICMPv6 o una cabecera IPv6 opcional.

- **Límite de saltos (8 bits):** Es el número de saltos máximo que le queda al paquete. El límite de saltos es establecido a un valor máximo por el origen y decrementado en 1 cada vez que un nodo enruta el paquete. Si el límite de saltos es decrementado y toma el valor de 0, el paquete es descartado.

- **Dirección origen (128 bits):** Es la dirección del origen del paquete.

- **Dirección destino (128 bits):** Es la dirección del destino del paquete.

Se puede observar, de los 12 campos de la cabecera de IPv4 se ha pasado a 8 campos en IPv6. El motivo fundamental por el que estos campos (tipo de servicio, indicadores, identificación y control de errores) son eliminados, es la innecesaria redundancia; en IPv4 se está facilitando la misma información de diversas formas, como es el caso del campo de control de errores, pues otros mecanismos de encapsulado de capas inferiores, por ejemplo IEEE 802 (estándares de redes de área local), ya realizan esta función.

El campo de desplazamiento de fragmentación de IPv4 ha sido eliminado, porque los paquetes ya no son fragmentados en los nodos intermedios, en IPv6 es un proceso que se produce extremo a extremo, el único campo realmente nuevo en IPv6 es la etiqueta de flujo.

A continuación se describe de forma más detallada los campos Clase de tráfico y etiqueta de flujo.

- Clase de tráfico: El campo de clase de tráfico de 8 bits permite a una fuente identificar las características en el tratamiento de tráfico que desea cada paquete relativo a otros paquetes de la misma fuente. La opción es permitir varias formas de servicios diferenciados, en el RFC 2466 se encuentran las siguientes directrices:

- La interfaz de servicio con IPv6 debe permitir a los protocolos de la capa superior proporcionar el valor del campo de clase de tráfico.

- Los nodos que permitan un uso específico del campo de clase de tráfico se les permite cambiar el valor de estos bits en los paquetes que ellos originan, reenvían o reciben, de acuerdo a como se requiera para ese uso específico.
- Un protocolo de la capa superior no debe suponer que el valor de los bits de clase de tráfico en un paquete recibido es el mismo que el que el valor enviado por la fuente del paquete.

- Etiqueta de flujo: El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen particular a un destino particular (anycast o multicast) y para el que, el origen desea un tratamiento especial por parte de los dispositivos de enrutamiento. Un flujo está unívocamente identificado por la combinación de una dirección origen y una etiqueta de flujo de 20 bits distinta de cero. Así, todos los paquetes que van a formar parte del mismo flujo tienen asignada por el origen la misma etiqueta de flujo.

Desde el punto de vista del origen, un flujo será normalmente una secuencia de paquetes que se generan por una única aplicación en el origen y tienen los mismos requisitos del servicio de transferencia, un flujo puede estar compuesto de una única conexión TCP o incluso de varias.

Y ahora haciendo referencia a los enrutadores, un flujo es una secuencia de paquetes que comparten atributos que afectan a cómo deben ser tratados por el enrutador. Estos incluyen atributos de camino, asignación de recursos, requisitos sobre cómo descartar, contabilidad de paquetes transmitidos y de seguridad.

Ninguna etiqueta de flujo tiene un significado especial; en consecuencia, el tratamiento especial que se ha de dar al flujo de paquetes se debe declarar de alguna forma.

2.4.2 Cabecera de extensión de IPv6

En IPv6, la información de capa internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguiente distinto, un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el campo Cabecera Siguiente de la cabecera precedente, las cabeceras de extensión deben ser procesadas en orden, ya que el contenido y semántica de cada una de ellas indican si se debe o no procesar la siguiente cabecera.

Cada cabecera de extensión tiene una longitud múltiplo entero de 8 octetos, con el fin de mantener el alineamiento de 8 octetos en las cabeceras siguientes. La razón de que los diferentes campos de la cabecera estén alineados a 64 bits, es que la nueva generación de procesadores, de 64 bits, pueda procesar dichos campos de una manera más eficiente.

En el estándar IPv6 se recomienda, que en el caso de que se usen varias cabeceras de extensión, deben aparecer en el siguiente orden:

1. Cabecera IPv6: Obligatoria debe aparecer siempre primero
2. Cabecera opciones salto-a-salto.
3. Cabecera de opciones para el destino: Para opciones a procesar por el primer destino que aparece en el campo dirección IPv6 de destino y por los destinos subsecuentes indicados en la cabecera de enrutamiento.

A continuación se definen los campos de la extensión de la cabecera IPv6, anteriormente se ha descrito el formato de la cabecera IPv6 por lo que se prosigue a las siguientes cabeceras.

2.4.3 Descripción de los campos de extensión de la cabecera

Cabecera opciones salto-a-salto

La cabecera de opciones salto-a-salto lleva información opcional que, sí está presente, debe ser examinada por cada dispositivo de enrutamiento a lo largo del camino. Esta cabecera contiene los siguientes campos:

- **Cabecera siguiente (8 bits):** Identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecera de extensión (8 bits):** Longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.

- **Opciones:** Campo de longitud variable que consta de una o más definiciones de opción. Cada definición se expresa mediante tres subcampos: tipo de opción (8 bits), que identifica la opción; longitud (8 bits), que específica la longitud en octetos del campo de datos de la opción; y datos de opción, que es una especificación de la opción de longitud variable. En la figura 2.6 se muestra la cabecera de opciones salto-salto.

En realidad se utilizan los cinco bits menos significativos del campo tipo de opción para especificar una opción particular. Los bits más significativos indican la acción que tiene que realizar un nodo que no reconoce el tipo de opción, de acuerdo a;

- 00-Ignorar esta opción y continuar procesando la cabecera.

- 01-Descartar el paquete.

- 10-Descartar el paquete y enviar un mensaje ICMP de problema de parámetro, código 2, a la dirección origen del paquete, indicando el tipo de opción no reconocida.

- 11-Dercartar el paquete y, solamente si la dirección destino del paquete no es una dirección multicast, enviar un mensaje ICMP de problema de parámetro, código 2, a la dirección origen del paquete, indicando el tipo de opción no reconocida.

El tercer bit específica si el campo de datos de la opción no cambia (0) o si puede cambiar (1) en el camino desde el origen al destino. Los datos que pueden cambiar se deben excluir de los cálculos de autentificación.

En el estándar IPv6, hasta ahora sólo se han especificado dos opciones: la opción de carga útil Jumbo y la opción de alerta al dispositivo de enrutamiento. La opción de carga útil Jumbo se utiliza para enviar paquetes con una carga útil

mayor de 65.535 octetos. El campo de datos de esta opción tiene una longitud de 32 bits, y da la longitud del paquete en octetos, excluyendo la cabecera IPv6. Para estos paquetes el campo de longitud de la carga en la cabecera IPv6 debe de estar a cero y no puede haber cabecera de fragmentación. Con esta opción, IPv6 permite tamaños de paquete de hasta 4 millones de octetos. Esto facilita la transmisión de paquetes de video grandes, y habilita a IPv6 a hacer el mejor uso de la capacidad disponible a través de cualquier medio de transmisión.

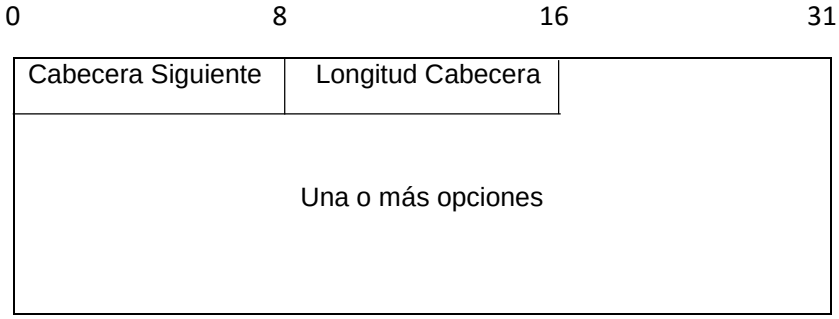


Figura 2.6 Cabecera de opciones salto-a-salto.

Cabecera de fragmentación

En IPv6, la fragmentación sólo puede ser realizada por el nodo origen, no por los dispositivos de enrutamiento a lo largo del camino del paquete. Para obtener las ventajas completas del entorno de interconexión, un nodo debe ejecutar un algoritmo de obtención de la ruta, lo que permite conocer la MTU permitida por cada red en la ruta. Con este conocimiento, el nodo origen fragmentará, según se requiera, para cada dirección destino dado. Si no se ejecuta este algoritmo, el origen debe limitar todos los paquetes a **1,280 octetos,** que debe ser la mínima MTU que permitan las redes. En la figura 2.7 se muestra la cabecera de Fragmentación.

La cabecera de fragmentación contiene los siguientes campos:

- **Cabecera siguiente (8 bits):** Identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Reservado (8 bits):** Para usos futuros.
- **Desplazamiento del fragmento (13 bits):** Indica donde se sitúa en el paquete original la carga útil de este fragmento. Se mide en unidades de 64 bits. Esto implica que los fragmentos (excepto el último) deben contener un campo de datos con una longitud múltiplo de 64 bits.
- **Reservado (2 bits):** Reservado para usos futuros.

- **Indicador M (1 bit):** 1= más fragmentos; 0= último fragmento.

- **Identificador (32 bits):** Utilizado para identificar de forma única el paquete original. El identificador debe ser único para la dirección origen, dirección destino y para el valor de la siguiente cabecera del paquete durante el tiempo que el paquete permanece en internet.

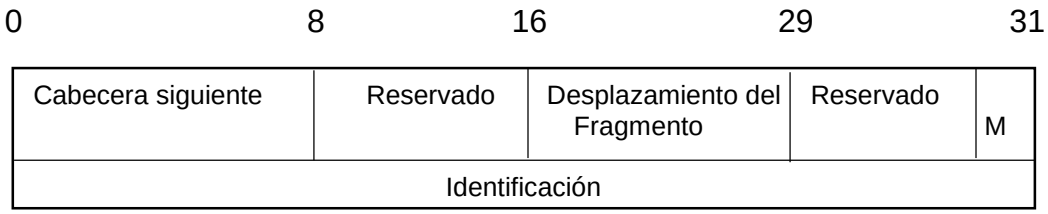


Figura 2.7 Cabecera de fragmentación

Cabecera de enrutamiento

La cabecera de enrutamiento contiene una lista de uno o más nodos intermedios, por los que se pasa en el camino del paquete a su destino. Todas las cabeceras de enrutamiento comienzan con un bloque de 32 bits consiste en 4 campos de 8 bits, seguido por datos de enrutamiento específicos al tipo de enrutamiento dado. En la figura 2.8 se muestra la cabecera de enrutamiento.

Los cuatro campos de 8 bits son los siguientes

- **Cabecera siguiente (8 bits):** Identifica el tipo de cabecera que sigue inmediatamente a ésta.

- **Longitud de la cabecera de extensión (8 bits):** Longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.

- **Tipo de enrutamiento (8 bits):** Identifica una variante particular de cabecera de enrutamiento. Si un dispositivo de enrutamiento no reconoce el valor del tipo de enrutamiento, debe de descartar el paquete.

- **Segmentos que quedan (8 bits):** Número de segmentos en la ruta que quedan; esto es, el número explícito de nodos intermedios en lista que se visitarán todavía antes de alcanzar el destino.

El único formato de cabecera de tipo enrutamiento explícito, definido en la Petición de Comentarios 2460 (RFC, por sus siglas en inglés, Request for Comments), es el

de la cabecera de enrutamiento tipo. Cuando se utiliza una cabecera de enrutamiento Tipo 0, el nodo origen no sitúa la dirección del último destino en la cabecera IPv6. En lugar de eso, esa dirección es la última de la lista en la cabecera de enrutamiento, y la cabecera IPv6 contiene la dirección destino del primer dispositivo de enrutamiento deseado en el camino, la cabecera de enrutamiento no se examina hasta que el paquete llega al nodo identificado por la cabecera IPv6. Es ese punto, el paquete IPv6 y el contenido de la cabecera se actualizan y el paquete es reenviado. La actualización consiste en situar la siguiente dirección a visitar en la cabecera IPv6 y decrementar el campo segmentos que quedan en la cabecera de enrutamiento.

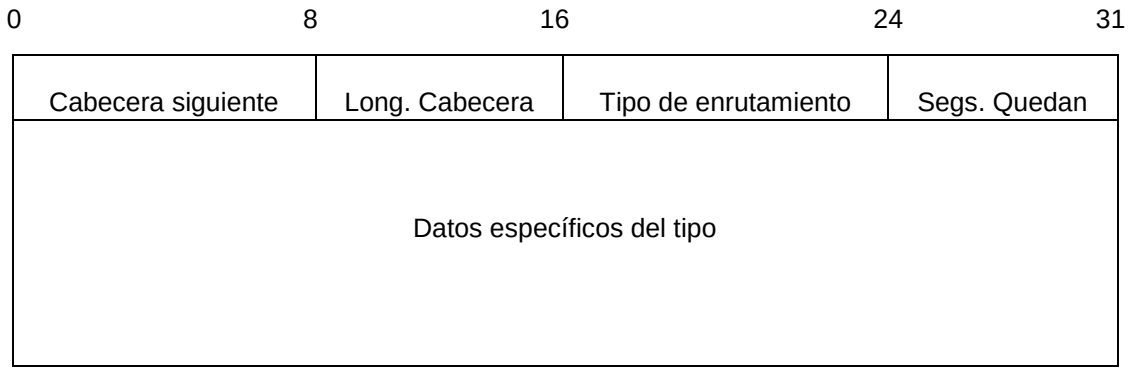


Figura 2.8 Cabecera de enrutamiento

Cabecera de opciones para el destino

La cabecera de opciones para el destino lleva información opcional que, si está presente, se examina por el nodo destino del paquete. El formato de esta cabecera es el mismo que la cabecera de opciones salto-a-salto. En la figura 2.9 se muestra la cabecera de opciones para el destino.

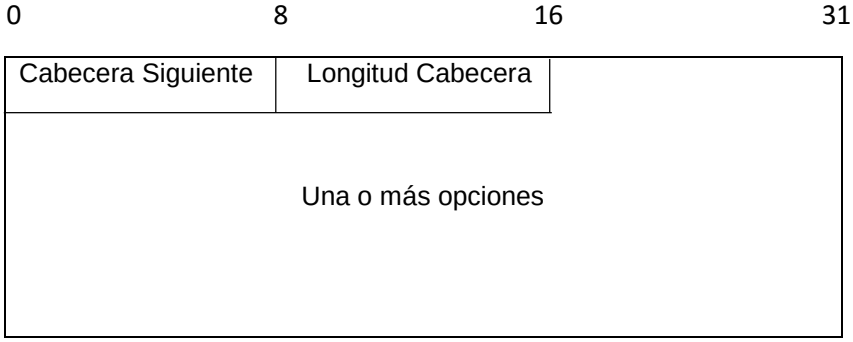


Figura 2.9 Cabecera de opciones para el destino.

2.5 Direccionamiento en IPv6

Las direcciones IPv6, descritas en el RFC 2373, soportan un número de bits que cuadruplica al utilizado por las de IPv4. Así, mientras el espacio de direccionamiento total en IPv4 es de 2^32 (4.294.967.296), en IPv6 lo es de 2^128 (340,282,366,920,938,463,463,374,607,431,768,211,456).

Las direcciones IPv6 de 128 bits identifican interfaces individuales o grupos de interfaces. Las direcciones IPv6, cualquiera que sea el tipo, se asignan a las interfaces, no a los nodos. Puesto que cada interfaz pertenece a un único nodo, cualquiera de las direcciones de interfaces unicast de ese nodo podría ser utilizada como un identificador del nodo. Una única interfaz puede tener múltiples direcciones IPv6 de cualquier tipo (unicast, anycast y multicast).

- **Unicast:** Las direcciones unicast identifican a una interfaz, es decir, un paquete enviado a una dirección unicast será entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

- **Anycast:** Las direcciones anycast identifican un grupo de interfaces, de forma que un paquete enviado a una dirección anycast será entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano según la distancia asignada en el protocolo de enrutamiento.

- **Multicast:** Las direcciones multicast identifican, al igual que las anycast, a un grupo de interfaces, pero un paquete enviado a una dirección multicast, es enviado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6, ya que ha sido reemplazada por multicast.

La representación de las direcciones IPv6 sigue el esquema x.x.x.x.x.x.x.x, donde x es un valor hexadecimal de 16 bits. No es preciso escribir los ceros a la izquierda de cada campo y, puesto que además pueden existir varias cadenas de ceros, permite la escritura de su abreviatura mediante el uso de "::", el cual presenta múltiples grupos de 16 bits a 0 binario. Por ejemplo la dirección FE80:0000:0000:01A8:D9FF:FE86:130B se simplifica de la siguiente manera FE80::1A8D9FF:FE86:130B.

El tipo específico de dirección IPv6 viene indicado por los primeros bits de la dirección. Este campo de longitud variable es denominado prefijo y permite conocer donde está conectado un determinado nodo. La dirección IPv6 se compone, por consiguiente, de un prefijo seguido de un identificador de nodo.

Las direcciones unicast globales agregables basadas en el proveedor, son utilizadas para comunicaciones globales en todo internet. Estas direcciones son semejantes a las direcciones IPv4 utilizando CIDR. Los tres primeros bits,

correspondientes al prefijo son 101. El resto de la dirección la forman los siguientes campos, de longitud variable hasta hacer un total de 128 bits:

- **Campo de registro:** Identifica a la entidad de internet de que asigna los identificadores a los proveedores de servicios.
- **Campo de proveedor:** Identifica a un determinado proveedor de servicios, el cual asigna parte de su espacio de direccionamiento a sus suscriptores.
- **Campo de subscriptor:** Diferencia a los distintos suscriptores conectados a internet a través de un mismo proveedor de servicio.
- **Campo de subred:** Especifica un grupo de nodos físicamente conectados en la red del subscriptor.
- **Campo de interfaz:** Caracteriza a una interfaz de entre todas las conectadas a una determinada subred.

Las direcciones unicast de uso local son direcciones que sólo tienen un ámbito de enrutamiento local, es decir, dentro de una red local o dentro de la red de una única compañía, y que podrían ser únicas local o globalmente. Se han definido dos tipos de direcciones locales:

- **Direcciones locales de enlace:** Se utilizan en un único enlace, con propósitos tales como la autoconfiguración de la dirección. Por ello, los enrutadores no pueden transmitir ningún paquete con direcciones locales de enlace en el origen o destino. Tienen el prefijo 1111 1110 10, luego tiene un campo de bits 0, y finalmente el campo que identifica a la interfaz.
- **Direcciones locales de sitio:** Se utilizan en un único sitio, sin la necesidad de un prefijo global. Por ello, los enrutadores no pueden retransmitir ningún paquete con direcciones locales de sitio en el origen o el destino fuera del sitio local u organización. Tienen el prefijo 1111 1110 11, luego un campo de bits a 0, un campo con el identificador de subred, y finalmente el identificador de interfaz.

En ambos tipos de direcciones locales el identificador de interfaz es un identificador que debe ser único en el dominio en el cual está siendo usado. En la mayoría de los casos este identificador utilizará la dirección de red de área local de 48 bits de ese nodo, por ejemplo, en el caso de una red Ethernet se utilizará la dirección MAC. La subred, para el caso de las direcciones locales de sitio, identifica una red determinada del sitio local u organización.

Las direcciones unicast especiales definidas en IPv6 son:

- **Dirección de auto entorno (loopback):** Es la: 1. No debe ser asignada a una interfaz física, ya que se trata de una interfaz virtual, es utilizada para pruebas y comunicaciones dentro de un mismo nodo. En IPv4 es cualquier tipo de dirección que comience por 127 en el primer octeto.

- **Dirección no especificada:** Es la ::, no debe ser asignada a ningún nodo, pues indica ausencia de dirección. Por ejemplo, se halla en el campo de dirección fuente, indica que el nodo está iniciándose y todavía no sabe cuál es su dirección.

- **Direcciones IPv6 compatibles con IPv4:** Se utilizan en un mecanismo de transición de IPv4 a IPv6 conocido por túneles dinámicos/automáticos, que consiste básicamente en el envío de paquetes IPv6 sobre infraestructura de enrutamiento IPv4 de forma totalmente transparente, mediante el encapsulamiento del paquete IPv6 en paquete IPv4. El formato de estas direcciones consiste en los primeros 96 bits a 0 y los otros 32 con la dirección IPv4.

- **Direcciones IPv6 proyectadas desde IPv4:** Se utilizan para representar las direcciones IPv4 en los nodos que sólo soportan IPv4, como direcciones IPv6. Es decir, permiten que los nodos que soportan IPv4, puedan seguir trabajando en IPv6. El formato de estas direcciones consiste en los primeros 80 bits a 0, los siguientes 16 bits a 1, y los últimos 32 bits con la dirección IPv4.

Las direcciones anycast (RFC 2526), utilizan cualquiera de los formatos de direcciones definidos para las direcciones unicast. De esta forma, las direcciones anycast son sintácticamente indistinguibles de las direcciones unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los cuales se les ha asignado esa dirección se deben configurar explícitamente para que sepan que se trata de una dirección anycast.

Las direcciones multicast (RFC 2375), tienen un prefijo de 1111 1111. Después, tienen un campo de bandera de 4 bits, de los cuales los tres primeros están reservados y deben ser inicializados a 0, el último bit puede estar a 0, lo cual indica una dirección multicast asignada permanentemente, ó a 1, si es una dirección multicast asignada transitoriamente. El campo que sigue al de banderas es también de 4 bits y se denomina ámbito del grupo de multicast (global, local de nodo, local de enlace, local de sitio, etc.). Finalmente, el campo de grupo de 112 bits, identifica el grupo de multicast.

2.6 Comparación entre IPv4 e IPv6

Como se pudo apreciar existen relevantes diferencias entre IPv4 e IPv6 enseguida se mencionan las principales discrepancias.

- **Direcciones:** En IPv4 las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes). Mientras que en IPv6, las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).

- **Fragmentación:** IPv4, la llevan a cabo los enrutadores y la computadora que realiza el envío. IPv6, la lleva acabo únicamente la computadora que realiza el envío.

- **Encabezado:** IPv4, incluye una suma de comprobación, mientras que en IPv6 no incluye una suma de comprobación.

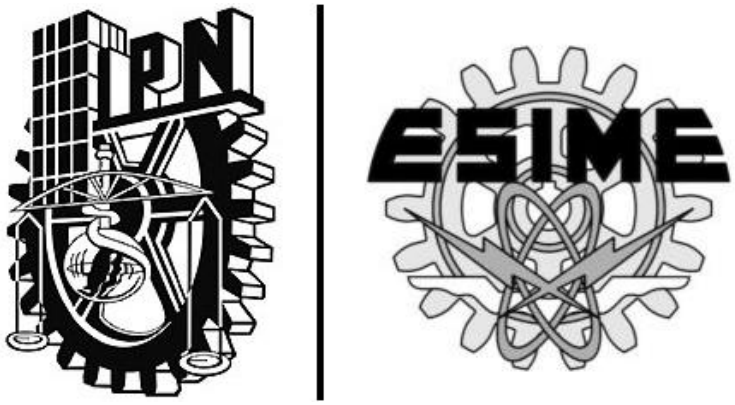
- **Direcciones de multicast:** En IPv4 se utilizan para enviar tráfico a todos los nodos de una subred. En IPv6, no hay direcciones de multicast, se utiliza una dirección de multicast para todos los nodos de una red local.

- **Configuración manual:** En IPv4 se debe configurar manualmente o a través de DHCP. En IPv6 no se requiere de configuración manual o a través de DHCP.

- **DNS:** IPv4 utiliza registros de recursos de direcciones de computadora en DNS para correlacionar nombres de computadora con direcciones IPv4. IPv6 utiliza los mismos recursos en DNS.

- **Tamaño de paquete:** IPv4 debe admitir un tamaño de 576 bytes con posible fragmentación e IPv6 se debe admitir un tamaño de 1280 bytes sin fragmentación.

- **Direccionamiento:** Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.



CAPÍTULO 3 | “Protocolos de Enrutamiento

Capítulo 3: Protocolos de Enrutamiento

3.1.- Principios Básicos de Enrutamiento

El enrutamiento pertenece a la capa de Red del Modelo OSI, este tiene la tarea de determinar la ruta o camino que deben seguir los paquetes a medida que fluyen de un emisor a un receptor. Los algoritmos que calculan estas rutas se conocen como algoritmos de enrutamiento. Un algoritmo de enrutamiento debe determinar, por ejemplo, la ruta por la que fluirán los paquetes desde el origen al destino.

El direccionamiento IP permite que los paquetes sean enrutados desde el origen al destino usando la mejor ruta posible. La propagación de paquetes, los cambios de encapsulamiento y los protocolos que están orientados a conexión y los que no lo están también son fundamentales para asegurar que los datos se transmitan correctamente a su destino.

En un conjunto de redes, los dispositivos de enrutamiento son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas. Cada dispositivo de encaminamiento realiza la decisión de enrutamiento basándose en el conocimiento que se tiene sobre la topología y las condiciones del conjunto de redes. En un conjunto de redes sencillo, es posible utilizar un esquema de enrutamiento fijo. En conjunto de redes más complejos, se necesita un grado de cooperación dinámica entre los dispositivos de enrutamiento. Para poder tomar decisiones de enrutamiento dinámico, los dispositivos de enrutamiento deben intercambiar información de enrutamiento usando un protocolo de enrutamiento especial para ese propósito.

Al considerar las funciones de enrutamiento de los dispositivos de encaminamiento hay que distinguir dos conceptos importantes:

- **Información de enrutamiento:** Información sobre la topología y el retardo del conjunto de las redes.

- **Algoritmo de enrutamiento:** Algoritmo utilizado para la toma de decisiones de encaminamiento para un datagrama particular, basándose en la información de encaminamiento actual.

3.1.1.- Métrica de Enrutamiento

Los algoritmos de enrutamiento utilizan métricas distintas para determinar la mejor ruta. Cada algoritmo de enrutamiento interpreta a su manera lo que es mejor. El algoritmo genera un número, denominado valor métrico, para cada ruta a través de la red. Los algoritmos de enrutamiento sofisticados basan la elección de la ruta en varias métricas, combinándolas en un sólo valor métrico compuesto. En general, los valores métricos menores indican la ruta preferida.

Las métricas pueden tomar como base una sola característica de la ruta, o pueden calcularse tomando en cuenta distintas características como:

- Ancho de banda: La capacidad de datos de un enlace. En general, se prefiere un enlace Ethernet de 10 Mbps a una línea arrendada de 64 kbps.

- Retardo: La cantidad de tiempo requerido para transportar un paquete a lo largo de cada enlace desde el origen hacia el destino El retardo depende del ancho de banda de los enlaces intermedios, de la cantidad de datos que pueden almacenarse de forma temporaria en cada Enrutador, de la congestión de la red, y de la distancia física

- Carga: La cantidad de actividad en un recurso de red como, por ejemplo, un Enrutador o un enlace.

- Confiabilidad: Generalmente se refiere al índice de error de cada enlace de red.

- Número de saltos: El número de enrutadores que un paquete debe atravesar antes de llegar a su destino. La distancia que deben atravesar los datos entre un enrutador y otro equivale a un salto. Una ruta cuyo número de saltos es cuatro indica que los datos que se transportan a través de esa ruta deben pasar por cuatro enrutadores antes de llegar a su destino final en la red. Si existen varias rutas hacia un mismo destino, se elige la ruta con el menor número de saltos.

- Tic-tacs: El retardo en el enlace de datos medido en tic-tacs de la computadora. Un tic-tac dura aproximadamente 1/18 de segundo.

- Costo: Un valor arbitrario asignado por un administrador de red que se basa por lo general en el ancho de banda, el gasto monetario u otra medida.

Métrica en los diferentes protocolos de enrutamiento

- RIP: La métrica utilizada por RIP es el número de saltos (hop count). Corresponde al número de enrutadores que deben atravesarse para alcanzar un destino. Para resolver los problemas de bucle, el número de saltos máximos es 15. Esto significa que una red cuyos paquetes puedan llegar a atravesar 16 enrutadores para alcanzar su destino, no puede utilizar el protocolo de enrutamiento RIP. Además de la utilización de una métrica limitada, los problemas de bucle se resuelven mediante las técnicas de horizonte dividido, de ruta inaccesible y de actualizaciones desencadenadas.

- IGRP e EIGRP: Utilizan ancho de banda, retardo, confiabilidad y carga; la mejor ruta se elige según la ruta con el valor de métrica compuesto más bajo calculado a partir de estos múltiples parámetros. Por defecto, sólo se usan el ancho de banda y el retardo.

- IS-IS y OSPF: Emplea costo; la mejor ruta se elige según la ruta con el costo más bajo.

Los protocolos de enrutamiento en un conjunto de redes funcionan de una forma similar a los que se utilizan en redes de conmutación de paquetes. Un protocolo de enrutamiento en un conjunto de redes se utiliza para intercambiar información sobre accesibilidad y retardos de tráfico, permitiendo a cada dispositivo de enrutamiento construir la tabla de enrutamiento del siguiente salto para los caminos a través del conjunto de redes.

3.1.2.-Distancia administrativa

La distancia administrativa es un número entero entre 0 y 255 que califica la confiabilidad de la información de enrutamiento recibida por un dispositivo de cualquiera de las fuentes de información disponibles. La distancia administrativa se utiliza como criterio de selección cuando el dispositivo tiene en su base de información múltiples rutas hacia el mismo destino, obtenidas a través de diferentes fuentes de información.

El algoritmo de selección de la mejor ruta establece que, ante rutas aprendidas de diferentes fuentes, se valorará como mejor ruta aquella que tenga menor distancia administrativa.

Para desarrollar esta tarea se asigna una distancia administrativa por defecto a cada fuente de información posible las cuales son:

- Red directamente conectada: 0
- Ruta estática: 1
- Ruta sumarizada EIGRP: 5
- eBGP: 20
- EIGRP (ruta interna): 90
- OSPF: 110
- IS-IS: 115
- RIP (v1 y v2): 120
- EIGRP (ruta externa): 170
- iBGP: 200

Cada protocolo usa su propio tipo de métrica para determinar la mejor ruta. No se puede realizar una comparación de las rutas con los diferentes tipos de métrica. Las distancias administrativas se ocupan de este problema. Las distancias administrativas tienen asignadas orígenes de rutas de manera que se elija la ruta del origen de preferencia como la mejor ruta.

Las distancias administrativas ayudan en la selección de rutas entre los diferentes protocolos de ruteo, pero pueden presentar problemas para la redistribución. Estos problemas pueden presentarse en la forma de bucles de ruteo, problemas de convergencia o ruteo ineficaz.

3.1.3.- Tablas de Enrutamiento

Los enrutadores utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo de enrutamiento utilizado. Las tablas de enrutamiento contienen la información necesaria para enviar paquetes de datos a través de redes conectadas.

Los dispositivos de Capa 3 interconectan dominios de broadcast o LAN. Se requiere un esquema de direccionamiento jerárquico para poder transferir los datos.

Los enrutadores mantienen información importante en sus tablas de enrutamiento, que incluye lo siguiente:

- Tipo de protocolo: El tipo de protocolo de enrutamiento que creó la entrada en la tabla de enrutamiento.

- Asociaciones entre destino/siguiente salto: Estas asociaciones le dicen al enrutador que un destino en particular está directamente conectado al enrutador, o que puede ser alcanzado utilizando un enrutador denominado "salto siguiente" en el trayecto hacia el destino final. Cuando un enrutador recibe un paquete entrante, lee la dirección destino y verifica si hay concordancia entre esta dirección y una entrada de la tabla de enrutamiento.

- Métrica de enrutamiento: Los distintos protocolos de enrutamiento utilizan métricas de enrutamiento distintas. Las métricas de enrutamiento se utilizan para determinar la conveniencia de una ruta. Por ejemplo, el número de saltos es la única métrica de enrutamiento que utiliza el protocolo de información de enrutamiento (RIP, por sus siglas en inglés, Routing Information Protocol).

- Interfaces de salida: La interfaz por la que se envían los datos para llegar a su destino final.

Los enrutadores se comunican entre sí para mantener sus tablas de enrutamiento por medio de la transmisión de mensajes de actualización del enrutamiento. Algunos protocolos de enrutamiento transmiten estos mensajes de forma periódica, mientras que otros lo hacen cuando hay cambios en la topología de la red.

Algunos protocolos (RIP, V1 y V2) transmiten toda la tabla de enrutamiento en cada mensaje de actualización, y otros transmiten sólo las rutas que se han modificado (OSPF). Un ruteador crea y guarda su tabla de enrutamiento, analizando las actualizaciones de enrutamiento de los enrutadores vecinos.

3.2.- Protocolos Enrutados

Un protocolo enrutado permite que un enrutador envíe datos entre nodos de diferentes redes. Para que un protocolo sea enrutable, debe admitir la capacidad

de asignar a cada dispositivo individual un número de red y uno de Host. Algunos protocolos como IPX, requieren sólo de un número de red porque estos protocolos utilizan la dirección MAC del dispositivo como número de Host. Otros protocolos, como IP, requieren una dirección completa que especifique la porción de red y la porción del dispositivo. Estos protocolos también necesitan una máscara de red para diferenciar estos dos números. La dirección de red se obtiene al realizar la operación "AND" con la dirección y la máscara de red.

La razón por la que se utiliza una máscara de red es para permitir que grupos de direcciones IP secuenciales sean considerados como una sola unidad. Si no se pudiera agrupar, cada dispositivo tendría que mapearse de forma individual para realizar el enrutamiento. Esto sería imposible, ya que de acuerdo al Consorcio de Programas de Internet (ISC) existen aproximadamente 233,101,500 host en Internet.

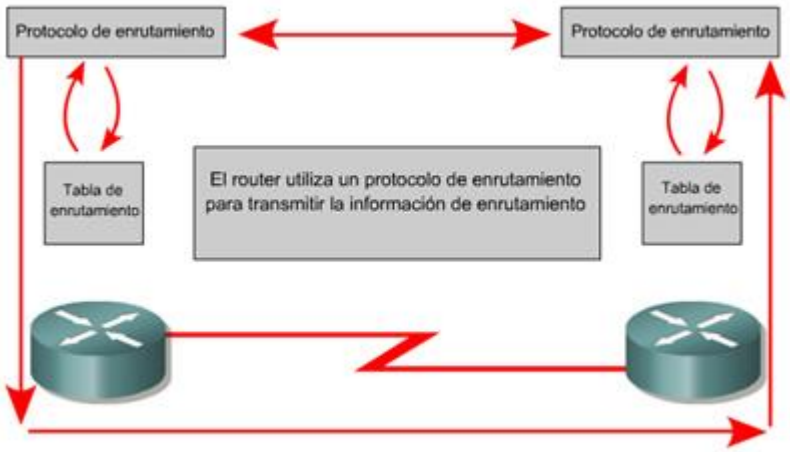


Figura 3.1 Ejemplo de un Protocolo de Enrutamiento

El Protocolo Internet y el intercambio de paquetes de internetworking (este término se utiliza para designar la unión de redes diferentes a cualquier nivel físico, de enlace, etc.) de forma que desde los niveles superiores se aprecie como una única red homogénea. Algunos ejemplos como Internetwork Packet Exchange (IPX) de Novell son ejemplos de protocolos enrutados. Otros ejemplos son, AppleTalk y Xerox Network Systems (XNS).

Los enrutadores utilizan los protocolos de enrutamiento para intercambiar las tablas de enrutamiento, que son aquellas que contienen un listado con todas las redes remotas con las que tiene constancia y así compartir la información de enrutamiento. En otras palabras, los protocolos de enrutamiento son los que actualizan las tablas

de enrutamiento ya que permiten enrutar protocolos enrutados, los cuales llevan la información del usuario (dirección lógica).

Los ejemplos de protocolos de enrutamiento que admiten el protocolo enrutado IP incluyen el Protocolo de Información de Enrutamiento y el Protocolo de Enrutamiento de la Compuerta de Enlace Interior, el Protocolo de la Primer ruta más Corta Libre (OSPF, por sus siglas en inglés, Open Shortest Path First) y el Protocolo de Compuerta de Enlace Fronterizo.

RIP: Permite a los enrutadores intercambiar su información sobre posibles destinos para calcular las rutas a lo largo de toda la red. Los destinos pueden ser redes o valores especiales que representan rutas por defecto (La ruta por defecto es una ruta estática que tiene como destino cualquier red posible). RIP no altera los datagramas IP y los encamina basándose únicamente en el campo de dirección destino.

- IGRP: Es un protocolo utilizado para el intercambio de información entre enrutadores. Lo que se encarga de hacer es buscar la mejor vía de envío mediante el algoritmo de métrica vector-distancia.

- OSPF: Es un protocolo que detecta las mejores rutas a destinos (accesibles). Puede percibir rápidamente cambios en la topología de un Sistema Autónomo (SA), y después de un pequeño periodo de convergencia, calcular nuevas rutas. OSPF no encapsula los paquetes IP, sino que los hace progresar basándose solamente en la dirección de destino.

- BGP: Permite el encaminamiento de los paquetes IP que se intercambian entre los distintos SA. Para ello, es necesario el intercambio de prefijos de rutas entre los diferentes SA de forma dinámica. Este tipo de operación proporciona comunicación fiable y esconde todos los detalles de la red por la que se pasa.

- EIGRP: Es un protocolo hibrido pues tiene elementos tanto de protocolos de vectores distancia como de estado de vínculos, situándose en dicha categoría, actualmente no es tan usado pues perdió mucha fuerza ante OSPF.

3.3.- Protocolos de Enrutamiento

Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes. Los computadores se comunican intercambiando mensajes de datos. Para aceptar y actuar sobre estos mensajes, los computadores deben contar con definiciones de cómo interpretar el mensaje.

El propósito de un protocolo de enrutamiento incluye:

- Descubrimiento de redes remotas
- Mantenimiento de información de enrutamiento actualizada
- Selección de la mejor ruta hacia las redes de destino
- Capacidad de encontrar una mejor nueva ruta si la ruta actual deja de estar disponible.

Los componentes por los que está formado un protocolo son:

- Estructuras de datos: algunos protocolos de enrutamiento usan tablas y/o bases de datos para sus operaciones. Esta información se guarda en la memoria de acceso aleatoria (RAM, por sus siglas en inglés, Random-Access Memory).

- Algoritmo: un algoritmo es una lista limitada de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar la mejor ruta.

- Mensajes del protocolo de enrutamiento: los protocolos de enrutamiento usan varios tipos de mensajes para descubrir enrutadores vecinos, intercambiar información de enrutamiento y otras tareas para aprender y conservar información precisa sobre la red.

Los protocolos de enrutamiento con frecuencia tienen uno a más de los siguientes objetivos:

- Optimización: La optimización describe la capacidad del algoritmo de enrutamiento de seleccionar la mejor ruta. La mejor ruta depende de las métricas y el peso de las métricas que se usan para hacer el cálculo.

- Simplicidad y bajo gasto: Cuanto más simple sea el algoritmo, más eficientemente será procesado por la unidad central de procesamiento (CPU) y la memoria del enrutador. Esto es importante ya que la red puede aumentar en grandes proporciones, como la Internet.

- Solidez y estabilidad: Un algoritmo debe funcionar de manera correcta cuando se enfrenta con una situación inusual o desconocida; por ejemplo, fallas en la parte física, condiciones de carga elevada y errores en la implementación.

- Flexibilidad: Un algoritmo de enrutamiento debe adaptarse rápidamente a una gran variedad de cambios en la red. Estos cambios incluyen la disponibilidad y memoria del enrutador, cambios en el ancho de banda y retardo en la red.

- Convergencia rápida: La convergencia es el proceso en el cual todos los enrutadores llegan a un acuerdo con respecto a las rutas disponibles. Cuando un evento en la red provoca cambios en la disponibilidad de los enrutadores, se necesitan actualizaciones para restablecer la conectividad en la red. Los algoritmos de enrutamiento que convergen lentamente pueden hacer que los datos no puedan enviarse.

Los enrutadores utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo de enrutamiento utilizado. Las tablas de enrutamiento contienen la información necesaria para enviar paquetes de datos a través de redes conectadas.

3.3.1.- Vector Distancia

El enrutamiento por vector distancia fue el primero en aparecer en el mundo de TCP/IP. La parte principal de todos los protocolos de enrutamiento de vectores distancia es alguna forma de coste total. El coste total más simple añade los saltos (la cuenta de saltos) entre un enrutador y una red, por eso, si tuviera un enrutador un salto más allá, el coste de esta ruta sería 1. Si estuviera dos saltos más allá, el coste seria 2.

No todas las conexiones de red son iguales. Un enrutador puede tener dos rutas de uno para una red, una que utilice una conexión rápida y otra lenta. Los administradores establecen la métrica de las rutas en las tablas de enrutamiento para reflejar la velocidad. Por eso, la ruta lenta de un salto, por ejemplo, puede

ofrecer una métrica de 10 en lugar de 1 predeterminado para reflejar el hecho de que se trata de una ruta lenta de un salto es 10, aunque solo tenga un salto.

El protocolo de enrutamiento de vector distancia calcula el coste total para llegar a un ID de red determinado y lo compara con el coste total de otras rutas para llegar al mismo ID de red. Posteriormente, el enrutador elige la ruta con el coste más bajo.

Para llevar a cabo esta tarea, los enrutadores utilizan un protocolo de enrutamiento vector de distancia que transfiere la tabla de enrutamiento a otro enrutador de la red WAN. Los protocolos de enrutamiento de vector distancia tienen un máximo en cuanto a su métrica (saltos).

Los ejemplos de los protocolos por vector-distancia incluyen los siguientes:

- **RIPv1:** La primera versión de, RIPv1, se desarrolló en los 80`s aunque sus predecesores datan de los años 60`s, época de los inicios de Internet. RIP cuenta un máximo de 15 saltos por lo que el enrutador no se comunicara con otro enrutador que este a más de 15 saltos. Esto acabo siendo un problema ya que la petición de una tabla de enrutamiento podría realizar un bucle de vuelta al enrutador inicial.

  RIPv1 envía una actualización cada 30 segundos. Esto también se convirtió en un gran problema porque todos los enrutadores de la red enviarían su tabla de enrutamiento a la vez, provocando una saturación de la red.
  Los enrutadores RIPv1 no tenían protección, quedando expuestos a que los piratas informáticos enviaran información falsa de tablas de enrutamiento.

- **RIPv2:** Este protocolo se comporta igual a su antecesor, pero resuelve bastantes problemas de seguridad aunque sigue teniendo 15 saltos como su versión anterior, las actualizaciones se establecen en intervalos al azar y se crea una autentificación del protocolo. La mayoría de enrutadores todavía admiten RIPv2 pero RIP tiene muchos problemas, especialmente, el tiempo de convergencia de las redes WAN de mayor tamaño, que las hace obsoletas salvo para pequeñas redes privadas WAN que tengan pocos enrutadores (16 enrutadores).

- **BGP:** Internet ha fijado un único protocolo para la comunicación entre SA el Protocolo de Compuerta de Enlace Fronteriza. Este es el “pegamento” de Internet ya que conecta todos los Sistemas Autónomos. BGP no tiene el mismo tipo de tablas de enrutamiento que se conocen, en su lugar, los

enrutadores BGP se configuran manualmente y revelan información recibida desde distintos enrutadores perimetrales de distintos sistemas autónomos.

BGP también sabe cómo gestionar una serie de situaciones únicas de Internet. Si un enrutador anuncia una nueva ruta pero dicha ruta no es fiable, la mayoría de los enrutadores BGP la ignoran.

3.3.2 Estado de enlace

Los protocolos de enrutamiento de estado de enlace se diseñaron para superar las limitaciones de los protocolos de enrutamiento vector distancia. Los protocolos de enrutamiento de estado de enlace responden rápidamente a las modificaciones en la red, enviando actualizaciones sólo cuando se producen las modificaciones. Los protocolos de enrutamiento de estado de enlace envían actualizaciones periódicas, conocidas como renovaciones de estado de enlace a rangos más prolongados; por ejemplo, 30 minutos.

Por lo general, los algoritmos de estado de enlace utilizan sus bases de datos para crear entradas de tablas de enrutamiento que prefieran la ruta más corta. Ejemplos de protocolos de estado de enlace son:

OSPF: Los usuarios más grandes de Internet utilizan OSPF en sus redes internas. Converge con una velocidad espectacular, más rápida, y es mucho más eficiente que RIP. Cuando se inician por primera vez enrutadores con la habilidad de OSPF, envían anuncios de estado de vínculos (LSA), llamados paquetes “Hola” que buscan otros enrutadores OSPF.

Una de las grandes diferencias entre OSPF y RIP es el coste de salto. Mientras que los saltos individuales tienen un coste de 1 en RIP, a menos que se cambie manualmente, en OSPF el coste se basa en la velocidad del vínculo. La fórmula es

100, 000,000/ancho de banda en bps

De modo que el coste de OSPF de un vínculo es 10BaseT es 100, 000,000/10, 000,000 = 10. A mayor rapidez del ancho de banda, menor coste.

Cuando los enrutadores OSPF envían “holas” LSA, intercambian esta información y actualizan las bases de datos de estado de vínculos. Los “holas” se envían a todos los enrutadores OSPF de la red. Dichos enrutadores conocen el estado de vínculo de los demás. Esto ocurre en tan solo segundos.

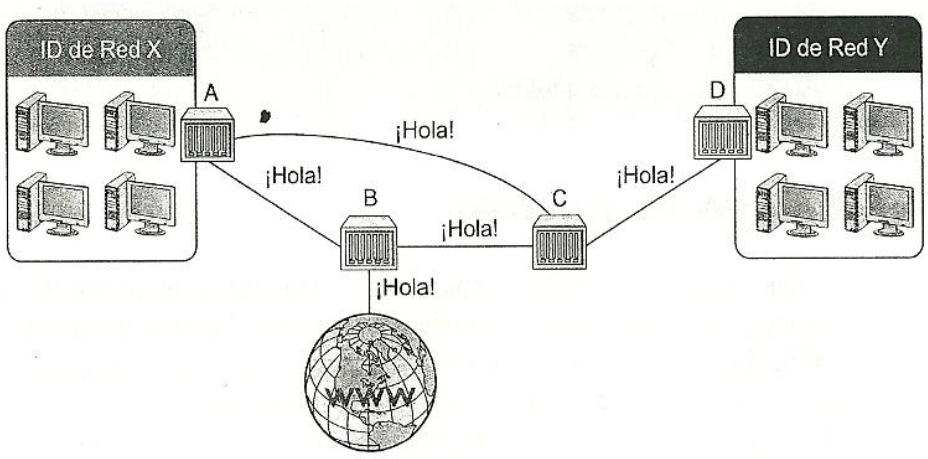


Figura 3.2 Mensajes hola en OSPF

Todos los enrutadores OSPF han sido diseñados para aceptar un Área ID. En este caso, todos los enrutadores tienen un Área ID de 0.0.0.0 (es muy similar a una dirección IP) que se conoce normalmente como Área 0.

El Área 0 es bastante importante en el mundo de OSPF. Si su red se va haciendo más compleja, pueden establecerse múltiples áreas. Sin embargo, el Área 0 es la más importante y, como tal, recibe el nombre de columna vertebral (backbone).

Una vez que se ha alcanzado la convergencia, todos los enrutadores del área se envían LSA “hola” cada 30 minutos o así a menos que detecten una interrupción en el estado de vínculos.

OSPF no es tan popular por casualidad, es fácil de utilizar, se adapta muy bien a redes de gran tamaño y lo admiten muy bien todos los enrutadores salvo los más básicos.

IS-IS: Si se quiere utilizar un protocolo de enrutamiento de estado de vínculos y no utiliza OSPF la única opción es IS-IS es cual es muy parecido a OSPF. Utiliza el concepto de áreas y solo envía actualizaciones a las tablas de enrutamiento. IS-IS se desarrolló prácticamente a la misma vez que OSPF y tuvo la gran surte de funcionar con IPv6 desde el principio. Lamentablemente ver cómo funciona IS-IS es muy difícil pues en la actualidad casi nadie lo ocupa.

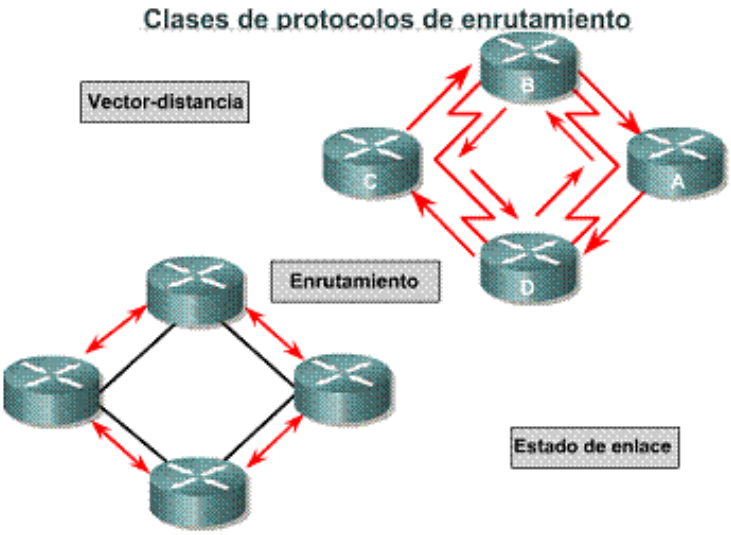


Figura 3.3 Ejemplo Vector distancia y Estado de Enlace

3.4.- Enrutamiento Estático y Dinámico

El enrutamiento es el proceso usado por el enrutador para enviar paquetes a la red de destino. Un enrutador toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los enrutadores deben aprender la ruta hacia las redes remotas. Cuando los enrutadores usan enrutamiento dinámico, esta información se obtiene de otros enrutadores. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios. En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una

ruta más confiable. Por lo tanto, es preferible instalar rutas de distancia administrativa menor antes que una ruta idéntica de distancia administrativa mayor. La distancia administrativa por defecto cuando se usa una ruta estática es 1. En la tabla de enrutamiento se observará la ruta estática indicando la interface de salida, como si hubiera conexión directa. Esto a veces confunde, ya que la redes directamente conectadas tienen distancia 0. Si el enrutador no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta. A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un enrutador, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

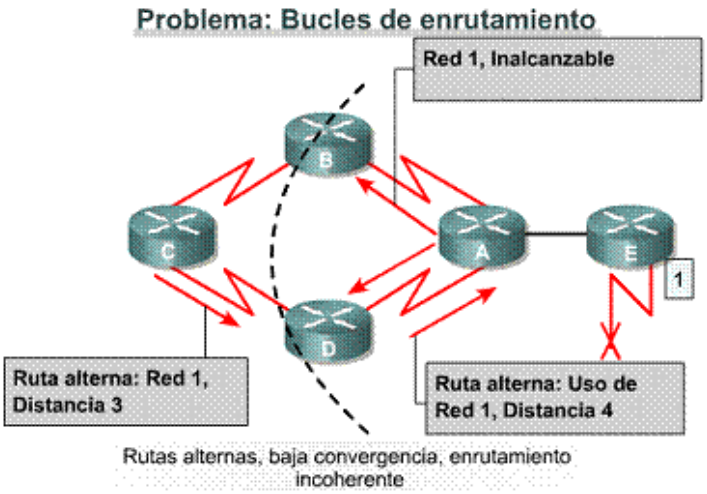
3.5.- Bucles de Enrutamiento

Los bucles de enrutamiento producen entradas de enrutamiento incoherentes, debido generalmente a un cambio en la topología. Si un enlace de un enrutador A se vuelve inaccesible, los enrutadores vecinos no se dan cuenta inmediatamente, por lo que se corre el riego de que el enrutador A crea que puede llegar a la red pérdida a través de sus vecinos que mantienen entradas antiguas. Así, añade una nueva entrada a su tabla de enrutamiento con un coste superior. A su vez, este proceso se repetirá una y otra vez, incrementándose el coste de las rutas, hasta que de alguna forma se parase dicho proceso.

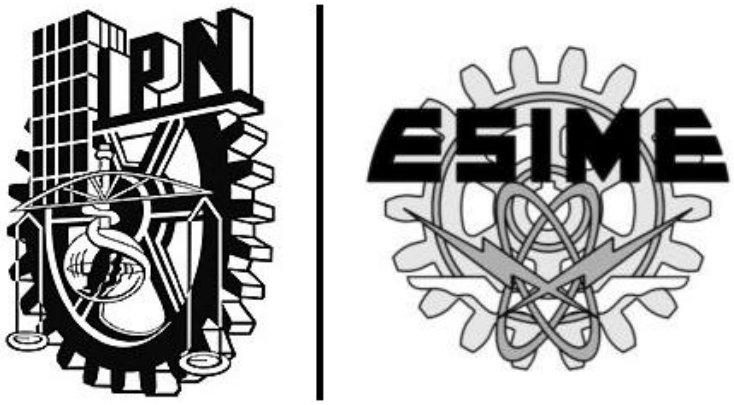
Los métodos utilizados para evitar este caso son los que siguen:

•Horizonte Dividido. La regla del horizonte dividido es que nunca resulta útil volver a enviar información acerca de una ruta a la dirección de dónde ha venido la actualización original.

•Actualización Inversa (Ruta envenenada): Cuando una red de un enrutador falla, este envenena su enlace creando una entrada para dicho enlace con coste infinito. Así deja de ser vulnerable a actualizaciones incorrectas proveniente de enrutadores vecinos, donde esté involucrada dicha red. Cuando los enrutadores vecinos ven que la red ha pasado a un coste infinito, se envía una actualización inversa indicando que la ruta no está accesible.



3.4. Bucles de enrutamiento



CAPÍTULO 4 | |“Desarrollo del Proyecto”

Capítulo 4: Desarrollo del Proyecto

En este capítulo se explica el protocolo de enrutamiento OSPF, el cual basa su funcionamiento a través de un algoritmo (Dijkstra), calculando la ruta más corta que debe recorrer un paquete desde el origen hasta el destino (Ruta de menor coste), el cual se explica detalladamente más adelante, el tipo de redes en las que opera y observar a fondo la cabecera de los mensajes que envía este protocolo para establecer una conexión.

Y de esta manera demostrar cómo se puede llegar a tener una coexistencia de IPv4 e IPv6, por medio del método de Doble Pila.

4.1. - OSPF

Este protocolo se usa frecuentemente como protocolo de encaminamiento interno de redes TCP/IP. Cuando se diseñó se quiso que cumpliera los siguientes requisitos:

- Ser abierto, en el sentido de que no fuera propiedad de una compañía.
- Que permita reconocer varias métricas, entre ellas, la distancia física y el retardo.
- Ser dinámico, es decir, que se adapte rápida y automáticamente a los cambios topológicos.
- Ser capaz de realizar un encaminamiento dependiendo del tipo de servicio.
- Implementar un mínimo de seguridad.

Para que pueda existir un mecanismo de transición de IPv4 a IPv6 antes se deben retomar otros temas que ayuden a tener una mejor visión de esta coexistencia, aunque ya se han abordado temas como los protocolos de enrutamiento, este capítulo se enfoca en particular al algoritmo OSPF del cual se describen sus características y su algoritmo de enrutamiento.

Se puede decir que OSPF, es un protocolo de estado. En lugar de procesar los caminos basándose en vectores de distancia, mantiene un mapa de topología de la red, lo cual ofrece una visión más global de la misma, y de esta forma es posible seleccionar los caminos más cortos.

OSPF está clasificado como un Protocolo de tipo Compuerta de Enlace Interior (IGP, por sus siglas en inglés, Interior Gateway Protocol) y fue diseñado para aceptar crecimientos en la red y poder difundir la información de encaminamiento de manera rápida. Entre otras las características más importantes son:

- Rápida detección de cambios en la topología de la red.
- Poca carga de la red, debido al envío de información correspondiente a los cambios sufridos en las rutas (en lugar de enviar las rutas completas).
- Capacidad de toma de decisiones. En los lugares en los que existen múltiples caminos, OSPF es capaz de hacer balance de decisiones.
- Decremento del tamaño de las tablas de rutas debido a la utilización de zonas como espacio de trabajo.
- Utilización de multienvío dentro de las áreas.
- Autenticación del intercambio de tablas de rutas.

Pero no todo son ventajas, OSPF también tiene algunos inconvenientes:

- Requiere una carga de proceso intensiva.
- Mantiene copias de la información de rutas, por lo que la cantidad de memoria requerida es amplia.
- Es un protocolo más complejo que RIP.

4.1.1.- Funcionamiento

Un Sistema Autónomo que utilice el protocolo OSPF está constituido por una o más áreas. Se entiende por área a un conjunto de redes y computadoras con sus correspondientes interfaces.

El área principal se denomina área 0 y está conectada a la red principal denominada red troncal, que se encarga de enlazar todas las áreas.

Los enrutadores de cada una de las áreas almacenan la información de enrutamiento. Esta información incluye la topología de la red, el estado de los

equipos de la red, enrutadores, etc. Mediante esta información es posible construir el mapa de área. Cuando ocurre un cambio en la red, la información se propaga por el área, permitiendo así que los enrutadores puedan saber si el acceso a una determinada red es posible o no.

Cuando un enrutador se conecta a la red, recibe de la computadora más cercana una copia sobre las tablas de encaminamiento, los siguientes envíos no serán más que las modificaciones que va sufriendo dicha tabla. Este tipo de envío se lleva a cabo mediante multicast. Para ello, cada enrutador genera una tabla más corta a través de las cuales se pueden alcanzar al resto de los enrutadores de la red, situándose él mismo como raíz de dicha jerarquía.

OSPF calcula diferentes rutas dependiendo del Tipo de Servicio, de manera que cuando existen rutas alternativas para alcanzar un destino, y cada una de estas rutas conlleva el mismo coste, OSPF distribuye el tráfico haciendo un balanceo de carga.

Una de las principales ventajas que conlleva el dividir cada Sistema Autónomo en áreas es que el protocolo OSPF trabaja con cada área de manera independiente. Un conjunto de redes son tratadas por OSPF como un área, y la topología de la misma se oculta del resto del Sistema Autónomo.

Esto reduce de manera considerable el tráfico de rutas dentro del Sistema Autónomo, así como permite una mayor flexibilidad a la hora de configurar la forma en que se va a llevar a cabo el intercambio OSPF. Debido a que cada intercambio de rutas OSPF es autenticado, es posible establecer un plan de autenticación para cada área de manera independiente.

Redes OSPF

El protocolo OSPF soporta los siguientes tipos de redes:

- Redes Punto a punto: Red que une dos enrutadores.
- Redes Broadcast: Son redes que soportan más de dos enrutadores y que tienen la posibilidad de enviar un único mensaje a todos los equipos conectados a ella.
- Redes No Broadcast: Redes que permiten más de dos enrutadores pero que no tienen la capacidad de envío en forma de broadcast.

Enrutadores OSPF

Cuando un Sistema Autónomo se divide en áreas, los enrutadores reciben también una clasificación especial:

- Enrutadores internos: Es un enrutador que enlaza dos redes dentro de una misma área o un enrutador con todas sus interfaces conectadas a la red troncal.

- Enrutadores de área: Enrutador que esta enlazado a diferentes áreas, la información sobre la topología de las áreas a las cuales está conectado es enviada por dicho enrutador a la red troncal.

- Enrutador troncales: Es un enrutador que tiene al menos una interfaz conectada a la red troncal, los enrutadores de área están incluidos en esta clasificación. Si un enrutador tiene todas sus interfaces conectadas a la red troncal y no solo una de ellas pasaría a denominarse enrutador interno.

- Enrutadores delimitadores de Sistema Autónomo: Es un enrutador que intercambia información con otros enrutadores que pertenecen a otros Sistemas Autónomos.

Para poder encaminar información fuera del área, los enrutadores de área envían información de las rutas dentro del área. Esta información incluye la topología del resto del Sistema Autónomo. El mecanismo mediante el cual se lleva a cabo tal labor es el siguiente:

Cada enrutador de área está conectado a la red troncal. Estos enrutadores realizan un esquema de la topología de las áreas que conectan para transmitir por la red troncal.

Cuando otro enrutador de área recibe la información proporcionada por su vecino, calcula los caminos más cortos hacia todos los destinos que no se encuentran dentro de las áreas conectadas a él.

El enrutador posteriormente encamina esta información hacia las áreas a las que está conectado, de esta forma cada uno de los enrutadores dentro de dichas áreas pueden escoger el mejor camino para enviar tráfico.

Mensajes OSPF

Los mensajes del protocolo OSPF se envían directamente encapsulados en datagramas IP. El protocolo OSPF fue diseñado para permitir la fragmentación de sus paquetes. Este nivel de fragmentación es preferible a la fragmentación realizada a nivel de red en los datagramas IP.

La cabecera de un mensaje de OSPF tiene el siguiente formato:

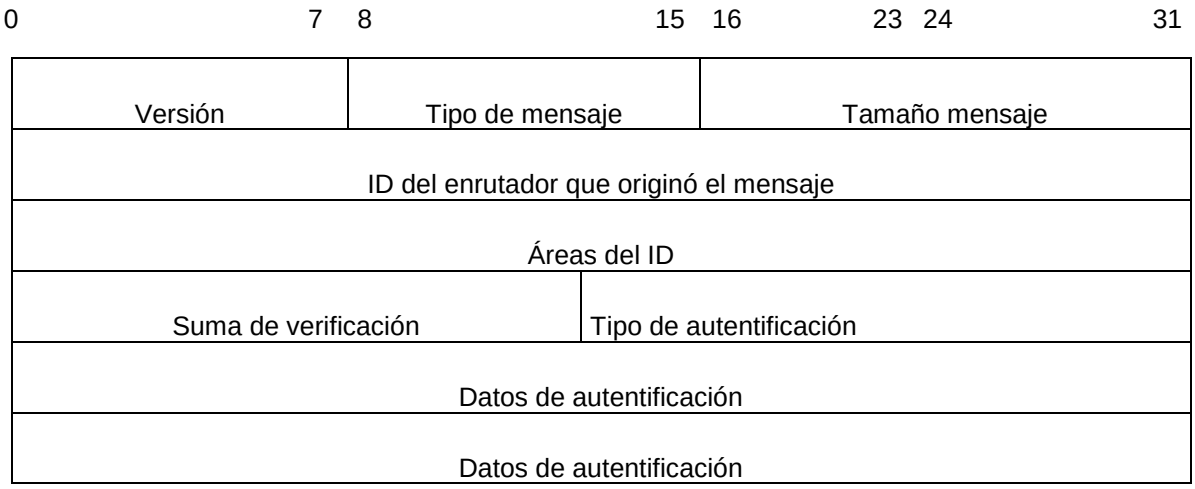


Figura 4.1 Cabecera de un mensaje OSPF

El primer campo del paquete indica la versión. En la actualidad es la versión 2 de OSPF.

El segundo campo es el tipo de mensaje. Puede ser los siguientes:

Tipo de Mensaje	Descripción
Saludo	Identifica los enrutadores vecinos, permite identificar un enrutador y enviar señales para notificar el correcto funcionamiento.
Descripción de las tablas de rutas	Intercambio de información de las tablas de rutas.
Petición del estado de enlace	Solicita datos que un enrutador no tiene en su tabla de rutas.
Actualización del estado enlace	Se utiliza como respuesta a los mensajes de petición del estado de enlace y para informar de los cambios en la topología de la red.
ACK del estado de enlace	Se utiliza para confirmar la recepción de una actualización del estado del enlace.

Tabla 4.1 Tipos de mensaje en OSPF

- El tercer campo indica el tamaño del mensaje incluyendo la cabecera.
- El cuarto campo es el número que identifica el enrutador que envía el mensaje.
- El quinto campo es el número de identificación del área donde se encuentra el enrutador.
- El sexto y séptimo campo son la suma de verificación y el tipo de autenticación.
- El resto de los campos tienen información sobre datos de autenticación.

Formato de los mensajes

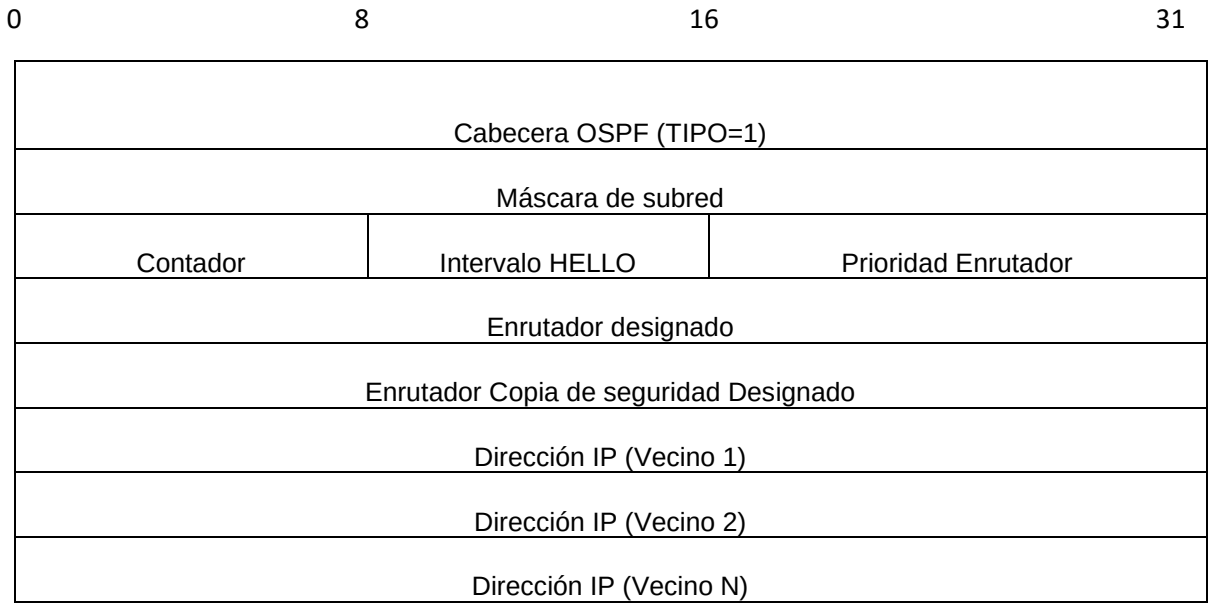


Figura 4.2.- Mensaje HELLO en OSPF

El protocolo OSPF envía de manera periódica el mensaje HELLO para que un enrutador verifique la accesibilidad con el enrutador vecino.

Los primero bytes del paquete son la cabecera explicada anteriormente, con la particularidad de que en el campo Tipo aparece el número 1, indicando que se trata de un mensaje HELLO.

El primer campo contiene la máscara de la red sobre la cual se está enviando el paquete.

El campo Contador contiene el tiempo, en segundos, tras el cual se considera sin actividad a un enrutador vecino que no está respondiendo.

El campo Intervalo HELLO es el periodo entre mensajes HELLO.

El campo Prioridad del Enrutador es un número que define la prioridad del enrutador. Este número tiene utilidad cuando es necesario definir un enrutador de copia de seguridad.

Los dos campos siguientes Enrutador Designado y Enrutador de copia de seguridad designado contienen las direcciones IP de dichos equipos.

El resto de los campos contienen las direcciones IP de los enrutadores vecinos, de los cuales, el emisor del mensaje ha recibido recientemente mensajes tipo HELLO.

Mensaje de descripción de las tablas de rutas

Este tipo de mensajes también recibe el nombre de mensajes de descripción de la base de datos, debido a que los enrutadores tienen una base de datos idéntica donde almacenan el estado de los equipos, enlaces, etc.

Esta base de datos puede ser muy amplia, en tal caso, para llevar acabo el intercambio de información, sería necesario enviar más de un paquete.

Tras la cabecera OSPF genérica aparece un campo Reservado, este campo debe tener todos sus bits, excepto los tres últimos, a cero.

Los bits I, M, S, tiene un significado especial cuando la base de datos es excesivamente grande y se requiere más de un mensaje.

Si I=1 se trata del mensaje inicial

Si M=1 indica que hay mensajes adicionales

Si S=1 indica que el enrutador que envía el mensaje es un maestro, en caso contrario se trata de un esclavo.

El campo Número de Secuencia de la base de datos numera los mensajes de manera secuencial, siendo el primer número uno aleatorio.

El campo Tipo Enlace puede tomar los valores siguientes:

Tipo Enlace	Descripción
1	Enlace Enrutador
2	Enlace de Red
3	Resumen de Enlace (red IP)
4	Resumen de Enlace (Para enrutador exterior)
5	Enlace Externo

Tabla 4.2.- Valores del campo Tipo Enlace.

- El campo ID Enlace contiene una identificación para el enlace.
- El campo Enrutador Notificador contiene la dirección IP del enrutador que envía el mensaje.
- El enrutador notificador genera un número de secuencia que permite asegurar que el mensaje no se recibe fuera de orden, este número se indica en el campo Número Secuencia de Enlace.
- La Suma de verificación permite verificar la integridad de los datos del paquete.
- El campo Tiempo Enlace es el tiempo en segundos transcurridos desde que se estableció el enlace.

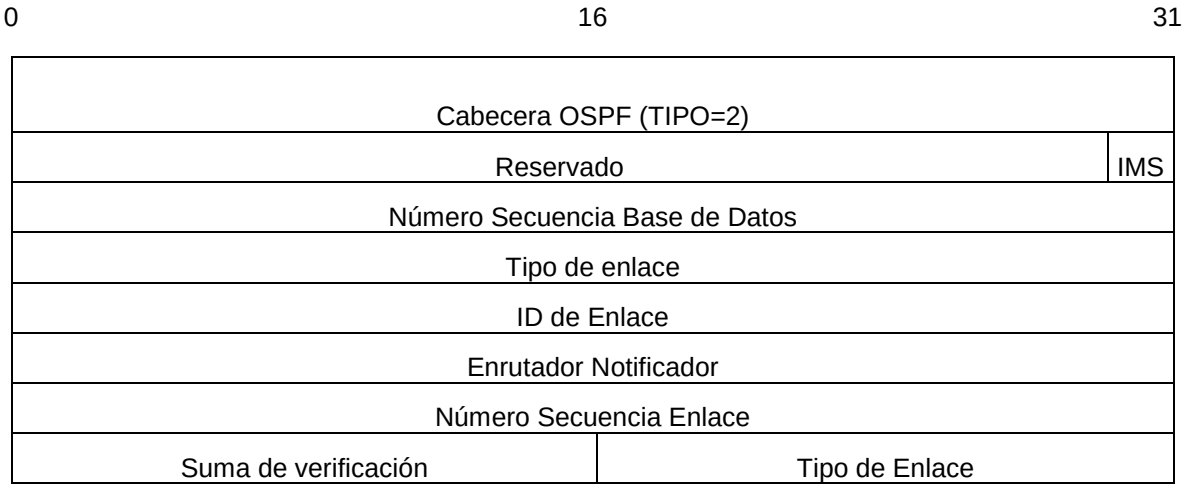


Figura 4.3.- Cabecera de un mensaje de descripción OSPF

Mensaje de solicitud del estado del enlace

En un momento determinado, un enrutador puede solicitar que le sea enviado un mensaje con la información sobre un determinado enlace. Este tipo de petición puede deberse a que la información que contiene en la base de datos está desfasada o simplemente es incoherente.

El formato del mensaje es el siguiente:

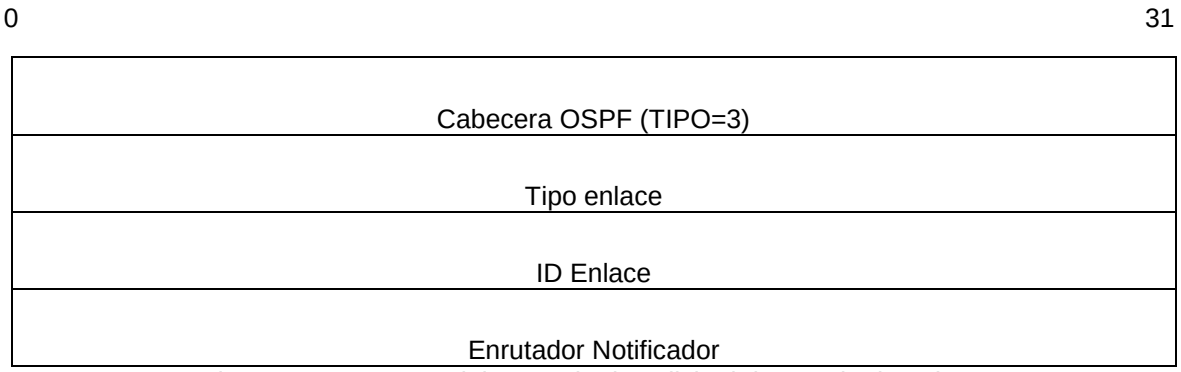


Figura 4.4.- Formato del mensaje de solicitud de estado de enlace

Mensaje de actualización del estado de enlace

Cada cierto tiempo, los enrutadores difunden un mensaje con las modificaciones que ha sufrido un enlace determinado. Este mensaje consiste en una serie de anuncios tal y como se muestra en la figura:

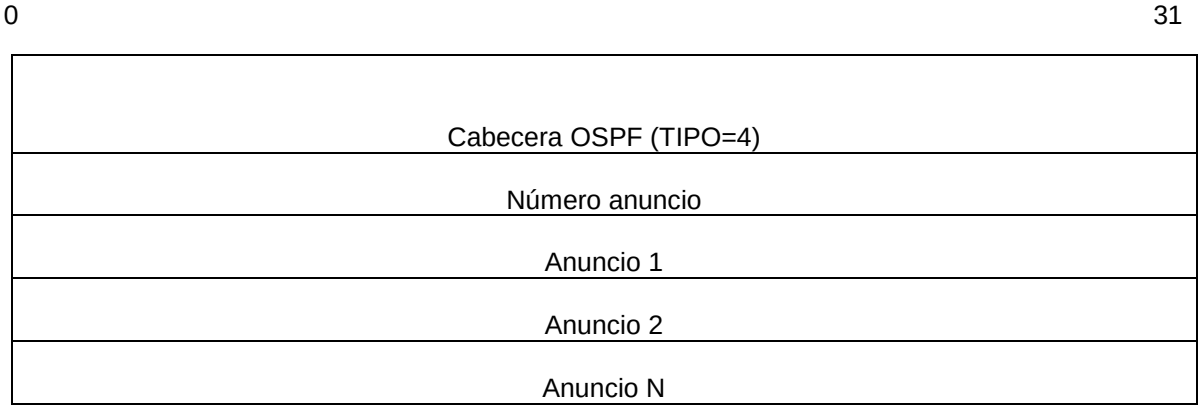


Figura 4.5.- Formato del mensaje de actualización de estado de enlace

4.1.2- Algoritmo OSPF Dijkstra

El algoritmo Dijkstra se puede enunciar de la siguiente manera: encontrar las rutas más cortas entre un nodo origen dado y todos los demás nodos desarrollando los caminos en orden creciente de longitud. El algoritmo actúa en dos pasos. En el paso k-ésimo se determinan los caminos más cortos a los k nodos más cercanos (de menor costo) al nodo origen; estos nodos se almacenan en el conjunto T. En el paso (k + 1) se añade a la lista T aquel nodo que presente el camino más corto desde el nodo origen y que no se encuentra ya incluido en la lista. A medida que se incorporan nuevos nodos a T, se define su camino desde el origen.

El algoritmo se puede describir formalmente como sigue:

- N = Conjunto de nodos de la red
- s = Nodo origen
- T = Lista o conjuntos de nodos añadidos o incorporados por el algoritmo
- w(i, j) = Coste del enlace desde el nodo i al nodo j; w(i, i) = 0, w(i, j) = ∞, si los dos nodos no se encuentran directamente conectados, w(i, j) ≥ 0 si los dos nodos están directamente conectados.
- L(n) = Coste en curso obtenido por el algoritmo para el camino de mínimo coste del nodo s al nodo n; al finalizar el algoritmo, este coste corresponde al del camino de mínimo coste de s a n en el grafo.

El algoritmo consta de 3 pasos, repitiendo los pasos 2 y 3 hasta que T = N; es decir, hasta que las rutas finales han sido asignadas a todos los nodos en la red:

1-. Inicio

T = {s} el conjunto de nodos incorporados sólo consta del nodo origen s

L(n) = w(i, j), con n ≠ s el coste inicial de las rutas a los nodos vecinos es el asociado a los enlaces.

2.- Obtención del siguiente nodo

Se busca el nodo vecino que no esté en T con el camino de menor coste desde s y se incorpora a T; también se incorpora el enlace desde ese nodo hasta un nodo en T que forma parte del camino.

Esto se puede expresar como:

Encontrar x ϵ T tal que L(x) = $\frac{min}{j \in T} L(j)$

Añadir x a T, incorporando también el enlace desde x que contribuye a L(x) como la componente de menor coste (es decir, salto en la ruta).

3.- Actualización de los caminos de coste

L(n) = min [L(n) + w(x, n)] ∀n ∄ T

Si el último término es el mínimo, el camino desde s hasta n es ahora el camino desde s hasta x concatenando con el enlace desde x hasta n.

El algoritmo concluye cuando todos los nodos han sido añadidos a T. Al final, el valor L(x) asociado a cada nodo x es el coste (longitud) de la ruta de mínimo coste de s a x. Además, T define el camino de mínimo coste desde s hasta cualquier otro nodo.

Cada iteración de los pasos 2 y 3 incorpora un nuevo nodo a T y define el camino de mínimo coste desde s hasta ese nodo, atravesando dicha ruta sólo nodos incluidos en T.

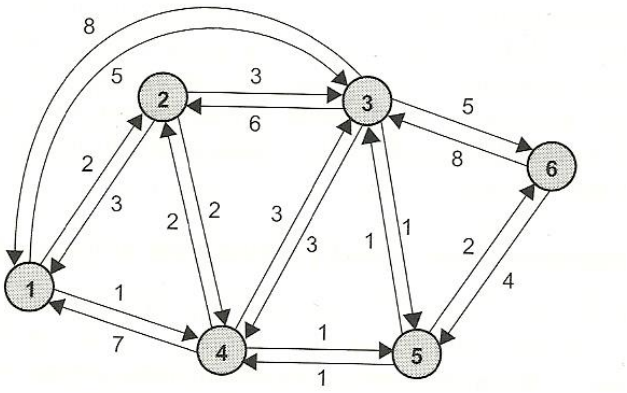


Figura 4.6.- Algoritmo Dijkstra

4.2.- Coexistencia entre IPv4 e IPv6

IPv6 fue diseñado para facilitar la transición y la coexistencia con IPv4. La técnica de transición de doble pila permite la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.

La migración de todas las computadoras conectadas a Internet de IPv4 a IPv6 es un proceso gradual. Los dos protocolos coexisten durante algún tiempo. La coexistencia en un sistema se garantiza donde se produce una implementación de doble pila en los dos protocolos.

Aún queda pendiente la cuestión de cómo se debe comunicar una computadora habilitada con IPv6 con un computadora IPv4 y cómo se debe transportar los paquetes IPv6 por las redes actuales, que normalmente se basan en IPv4.

Para facilitar el proceso de coexistencia se desarrollaron algunas técnicas que buscan mantener la compatibilidad de las redes que están desplegadas en IPv4 con el nuevo protocolo IPv6.

La clave para una transición exitosa está en la compatibilidad con la gran base instalada de computadoras y enrutadores IPv4. Al mantener la compatibilidad con IPv4 mientras se distribuye IPv6 se mejora la tarea de migrar el internet hacia IPv6.

Ese mismo documento especifica dos mecanismos de compatibilidad con IPv4 que pueden ser implementados en computadoras y enrutadores IPv6.

Doble capa IP (también conocido como doble pila). Una técnica que provee soporte completo para los protocolos de Internet: IPv4 e IPv6, en computadoras y enrutadores.

4.2.1.- Método Doble Pila

El método involucra que corran pilas de protocolos IPv4 e IPv6 sobre equipos de red tales como computadoras y enrutadores hasta que la transición a una red puramente IPv6 pueda ser terminada.

Cuando las dos pilas son utilizadas en los nodos conectados a las redes en los cuales ambos protocolos están habilitados simultáneamente, el método doble pila provee a los nodos la flexibilidad para establecer sesiones extremo a extremo sobre IPv4 o IPv6.

- Nodo IPv6/IPv4: Un "computadora" o "enrutador" que implementa IPv4 e IPv6.

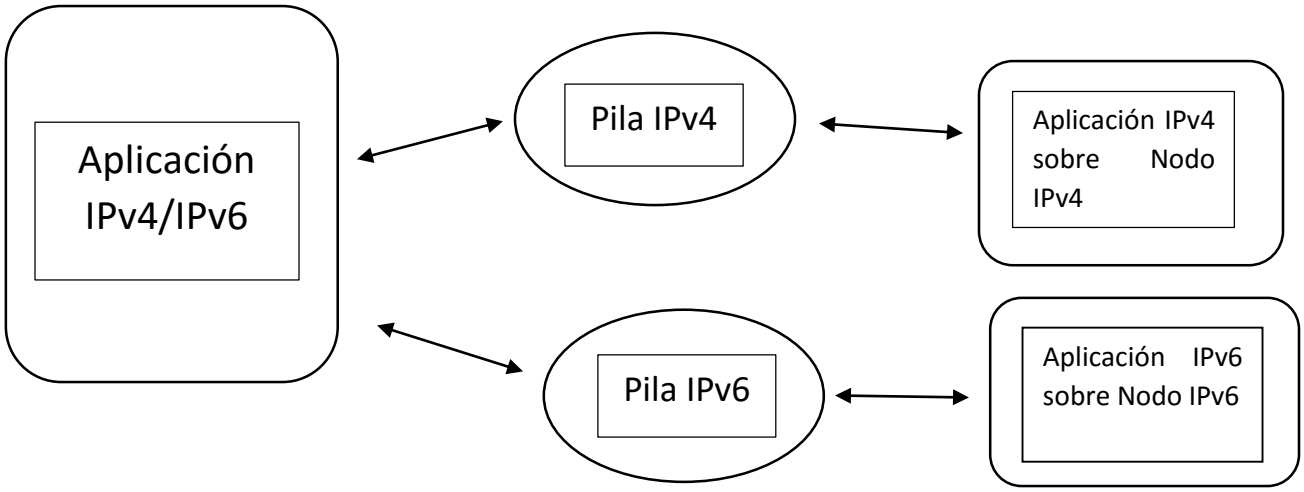


Figura 4.7 Método Doble Pila

El término doble pila normalmente se refiere a una duplicación completa de todos los niveles en la pila de protocolos desde la capa de aplicaciones a la de red. Un ejemplo de duplicación completa son los protocolos OSI y TCP/IP que corren en el mismo sistema.

Sin embargo, en el contexto de la transición IPv6, doble-pila significa que una pila de protocolo que contiene tanto IPv4 como IPv6. El resto de la pila es idéntico. Consecuentemente, los protocolos de transporte TCP, UDP etc., pueden correr tanto en IPv4 como IPv6. También las mismas aplicaciones pueden correr tanto en IPv4 como en IPv6.

La figura siguiente ilustra el mecanismo de doble pila en relación a la pila IPv4:

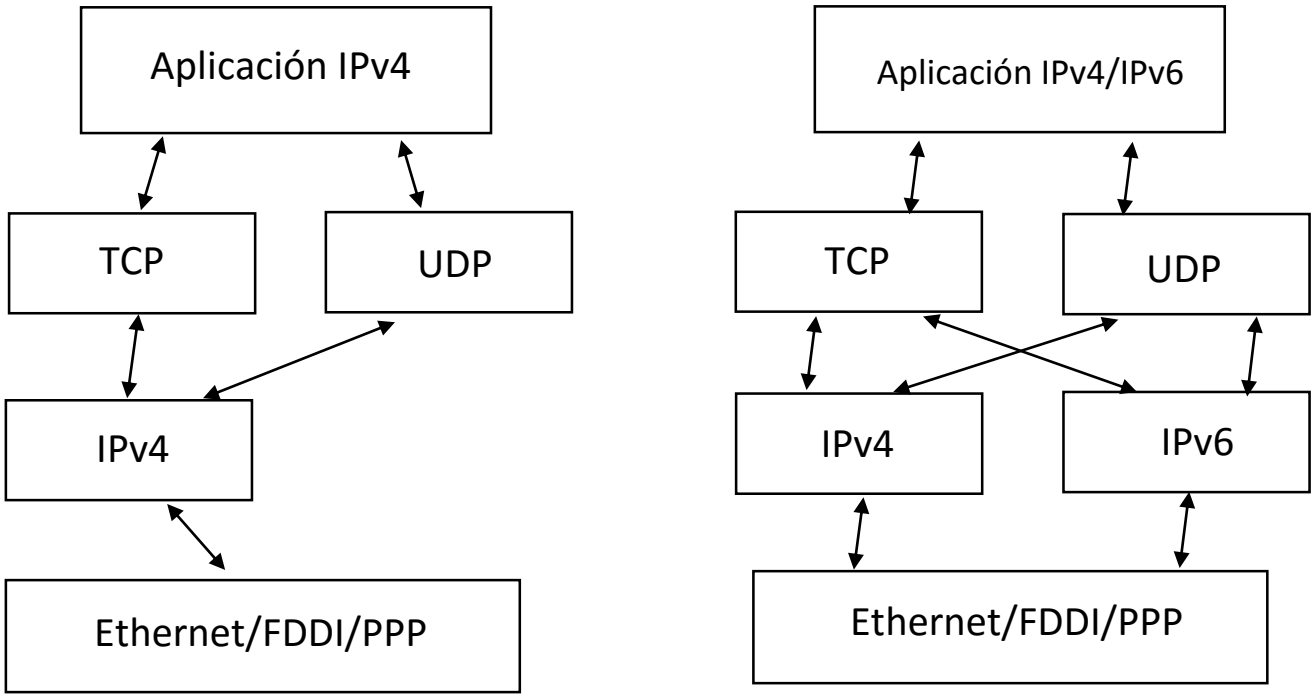


Figura 4.8 Doble Pila IPv4/IPv6 en relación a la pila IPv4 (Ethernet)

Cada nodo IPv4/IPv6, es configurado con direcciones IPv4 e IPv6. De ahí que pueda enviar y recibir datagramas que pertenecen a ambos protocolos y de ahí que se puedan comunicar con cada nodo en la red IPv4 e IPv6. Esta es la manera más simple y más deseable para que IPv4 e IPv6 coexistan y es más probable que sea el próximo paso en la evolución de una red en general, antes de que una transición más amplia a una Internet de sólo IPv6 pueda ser lograda a lo largo del mundo (en el largo plazo).

El modelo requiere que los “computadoras” y “enrutadores” implementen tanto IPv4 como lPv6. “Lo cual hace posible que las redes soporten servicios y aplicaciones de IPv4 e IPv6 durante el periodo de transición en el cual los servicios de IPv6 emergen y las aplicaciones de IPv6 se vuelvan disponibles”. Dependiendo sobre cual nodo se esté hablando, la aplicación usará IPv4 o IPv6 como la apropiada.

Esto puede ser determinado por la respuesta del DNS a un nombre de nodo. Si el DNS regresa una dirección IPv4, ésta se usa, si regresa una dirección IPv6, ésta se utiliza.

Se requiere de una infraestructura de DNS para la coexistencia exitosa, debido al uso prevalente de nombres en lugar de direcciones para referirse a los recursos de red. Actualizar esa infraestructura consiste de poblar los servidores de DNS con registros que soporten las resoluciones IPv6 de nombre a dirección y de dirección a nombre.

Después que las direcciones son obtenidas usando una consulta de nombres DNS, el nodo enviado debe seleccionar cuáles direcciones son usadas para la comunicación.

4.2.2.- Ventajas del modelo Doble Pila

Las ventajas del Mecanismo de Transición de Doble Pila:

- Los computadoras doble pila sobre redes IPv6 pueden alcanzar nodos IPv4 en la Internet Global. Estar en un ambiente sólo v6 no aísla a las computadoras del resto del Internet.

- Las aplicaciones tradicionales IPv4 pueden estar corriendo sobre redes sólo-IPv6. A todo el tráfico IPv4 se le realiza un túnel (IPv4 sobre IPv6) hacia la compuerta de enlace del mecanismo de transición de doble pila.
- Se reduce la necesidad de direcciones IPv4 globales. Una dirección es dada a la computadora sobre una base temporalmente solamente cuando tal dirección es necesitada.
- Cualquier tipo de protocolo/aplicación puede ser transparentemente avanzado. No necesitan configurarse traductores.

4.2.3.- Problemas Doble Pila

Los problemas en la operación del DHCP en la doble pila son:

- Manejo de respuestas múltiples. Surge la pregunta de cómo manejar información que puede ser recolectada desde fuentes múltiples.
- Diferente manejo administrativo. Los servicios de IPv4 e IPv6 pueden no estar administrados por la misma organización.
- Balanceo de cargas en el DNS.

- Problemas en la trayectoria de búsqueda del DNS. La trayectoria de búsqueda puede variar por razones administrativas
- Secuencia de arranque del protocolo. Se necesita considerar que sucede si la interfaz IPv6 es iniciada después de que DHCPv4 fue usada para configurar el cliente.
- Variaciones de opciones de DHCP. Algunas opciones en DHCP no están disponibles en DHCPv6 y viceversa.
- Problemas de seguridad. Los servidores DHCP y DHCPv6 son susceptibles a ser atacados.

4.3.- Resultados

Ahora se muestran los resultados obtenidos durante el proyecto, desde la implementación de direcciones IPv4 como IPv6 pasando por el método doble pila, finalmente se mostraran los protocolos del modelo TCP/IP que existen durante la coexistencia de IPv4 e IPv6.

Para el desarrollo del proyecto se utilizó una Red Delta, en la cual por fines de confidencialidad no se ocuparan las direcciones IP reales, solo se hará mención de los nombres de los nodos que conforman la misma.

Para poder realizar la coexistencia de estos dos protocolos es necesario establecer una red delta, habiendo que configurar cada uno de los nodos con sus respectivas direcciones y declarando el protocolo de enrutamiento que servirá para establecer una conexión entre ellos, una vez configurada la red se agregan 3 ordenadores a los cuales también hay que configurarles sus direcciones y que tengan una conexión con los nodos de la delta, una vez establecido esto se procede a realizar la prueba del método doble pila.

Para poder llevar a cabo la prueba es necesario hacer uso del símbolo del sistema del ordenador para hacer pruebas de “PING” y de la instrucción “Tracert” los cuales ayudan a saber si existe una comunicación entre nodos y que caminos toman los paquetes de datos en los protocolos de IPv4 e IPv6.

4.3.1.- Diagrama de la Red

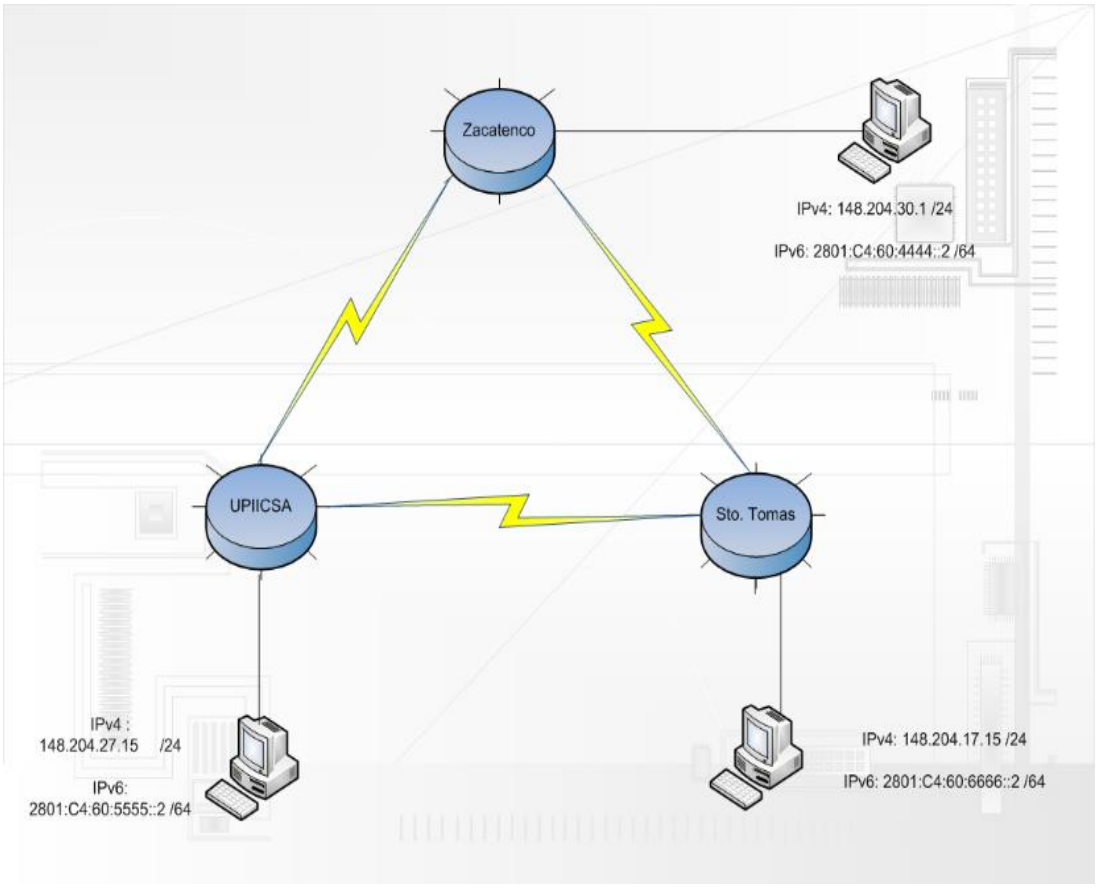
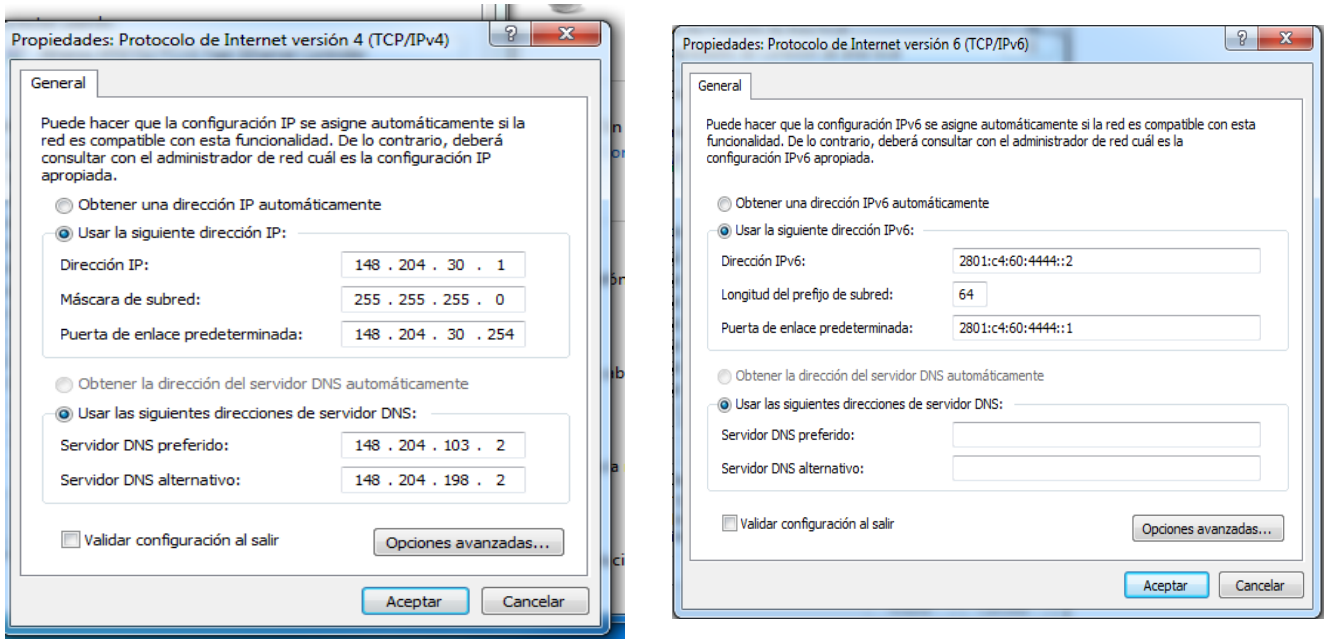


Figura 4.9.- Red

Las siguientes imágenes muestran la configuración de direcciones IPv4 e IPv6.



a) Dirección IPv4 b) Dirección IPv6

Figura 4.10.- Asignación de Direcciones IPv4 e IPv6 en los ordenadores.

En el inciso a) se muestra la configuración del direccionamiento IPv4, la cual se compone por: dirección IP, mascara de subred y compuerta de enlace; y en el inciso b) se observa la misma configuración solo que el formato de direccionamiento es en IPv6, la dirección IP y la compuerta de enlace predeterminada esta en formato hexadecimal y la longitud del prefijo de subred es de 64 bits. Cabe mencionar que la configuración antes mencionada fue empleada para cada enrutador de la delta.

La dirección ocupada para el nodo Zacatenco en IPv4 es 148.204.30.1/24 y en IPv6 es 2801:c4:60:4444::2/64

La dirección ocupada para el nodo UPIICSA en IPv4 es 148.204.27.15/24 y en IPv6 es 2801:c4:60:5555::2/64

La dirección ocupada para el nodo Santo Tomas en IPv4 es 148.204.17.15/24 y en IPv6 es 2801:c4:60:6666::2/64

4.3.2.- Configuración de enrutadores y tablas de enrutamiento

Ya que se tiene un esquema de la red se procede a configurar los enrutadores con las direcciones antes mencionadas, para hacer esto desde algún ordenador es necesario un emulador de terminal el cual permite por medio de instrucciones configurar el enrutador y establecer las conexiones necesarias para una comunicación.

En el siguiente código se muestra la configuración del enrutador “Zacatenco” con las direcciones IPv4 e IPv6, después se puede apreciar las tablas de enrutamiento de los enrutadores que ya están configurados con ambos protocolos IP:

```
! Last configuration change at 22:21:40 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:46:58 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:46:58 UTC Fri Feb 28 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
computadoraname Zacatenco
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
license udi pid CISCO2911/K9 sn FTX1628A04W
!
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 148.204.5.1 255.255.255.0
 duplex auto
 speed auto
```

Indica la interfaz en la cual está alojada la dirección IP

```
 ipv6 address 2801:C4:60:1111::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 148.204.15.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:3333::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/2
 ip address 148.204.30.254 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:4444::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
enrutador ospf 1
 network 148.204.5.0 0.0.0.255 area 0
 network 148.204.15.0 0.0.0.255 area 0
 network 148.204.30.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 enrutador ospf 1
 enrutador-id 1.1.1.1
¡
control-plane
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

En esta parte se puede ver ya establecidas las dos direcciones IP el tipo de protocolo de enrutamiento que se uso.

Direcciones IPv4 configuradas con el protocolo de enrutamiento OSPF.

```
Zacatenco#
Zacatenco#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2801:C4:60:1111::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2801:C4:60:1111::1/128 [0/0]
     via GigabitEthernet0/0, receive
O   2801:C4:60:2222::/64 [110/2]
     via FE80::D68C:B5FF:FE1B:9BA8, GigabitEthernet0/1
C   2801:C4:60:3333::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2801:C4:60:3333::2/128 [0/0]
     via GigabitEthernet0/1, receive
C   2801:C4:60:4444::/64 [0/0]
     via GigabitEthernet0/2, directly connected
L   2801:C4:60:4444::1/128 [0/0]
     via GigabitEthernet0/2, receive
O   2801:C4:60:5555::/64 [110/3]
     via FE80::D68C:B5FF:FE1B:9BA8, GigabitEthernet0/1
O   2801:C4:60:6666::/64 [110/2]
     via FE80::D68C:B5FF:FE1B:9BA8, GigabitEthernet0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

Figura 4.11.- Tabla de Enrutamiento Zacatenco

```
UPIICSA#
UPIICSA#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2801:C4:60:1111::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2801:C4:60:1111::2/128 [0/0]
     via GigabitEthernet0/1, receive
C   2801:C4:60:2222::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2801:C4:60:2222::1/128 [0/0]
     via GigabitEthernet0/0, receive
O   2801:C4:60:3333::/64 [110/2]
     via FE80::D68C:B5FF:FE1B:9BA9, GigabitEthernet0/0
O   2801:C4:60:4444::/64 [110/3]
     via FE80::D68C:B5FF:FE1B:9BA9, GigabitEthernet0/0
C   2801:C4:60:5555::/64 [0/0]
     via GigabitEthernet0/2, directly connected
L   2801:C4:60:5555::1/128 [0/0]
     via GigabitEthernet0/2, receive
O   2801:C4:60:6666::/64 [110/2]
     via FE80::D68C:B5FF:FE1B:9BA9, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Figura 4.12.- Tabla de Enrutamiento UPIICSA

```
StoTomas#
StoTomas#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2801:C4:60:1111::/64 [110/2]
     via FE80::A693:4CFF:FEF8:69A9, GigabitEthernet0/0
C   2801:C4:60:2222::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2801:C4:60:2222::2/128 [0/0]
     via GigabitEthernet0/1, receive
C   2801:C4:60:3333::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2801:C4:60:3333::1/128 [0/0]
     via GigabitEthernet0/0, receive
O   2801:C4:60:4444::/64 [110/2]
     via FE80::A693:4CFF:FEF8:69A9, GigabitEthernet0/0
O   2801:C4:60:5555::/64 [110/2]
     via FE80::D68C:B5FF:FE53:A860, GigabitEthernet0/1
C   2801:C4:60:6666::/64 [0/0]
     via GigabitEthernet0/2, directly connected
L   2801:C4:60:6666::1/128 [0/0]
     via GigabitEthernet0/2, receive
L   FF00::/8 [0/0]
     via Null0, receive
StoTomas#
```

Figura 4.13.- Tabla de Enrutamiento Santo Tomas

Para poder apreciar la tabla de enrutamiento se necesita de la instrucción “show ipv4/6 route” para que despliegue en pantalla las imágenes ya antes vistas, las cuales indican las computadoras que se encuentran directamente conectadas y las que están usando el protocolo de enrutamiento OSPF.

4.3.3.- Pruebas de Ping

Para saber si los enrutadores están teniendo comunicación entre ellos se solicita mediante la instrucción “Ping” la cual le envía paquete de datos para ver si la dirección destino los está recibiendo y existe una comunicación entre enrutadores.

Los enrutadores responden con unas estadísticas que indican el número de paquetes enviados, recibidos y perdidos con un tiempo de vida, si los paquetes enviados son igual a los recibidos existe una comunicación entre enrutadores por el contrario si los paquetes enviados son igual a los perdidos no existe una comunicación entre los enrutadores.

El tiempo de vida controla el tiempo máximo que el datagrama puede permanecer en la red hasta su llegada al destino. Si el tiempo se agota antes de finalizar el

camino, el datagrama es eliminado por el enrutador que detecta la situación. El campo es inicializado por la computadora de origen y va decrementándose en cada uno de los enrutadores del camino.

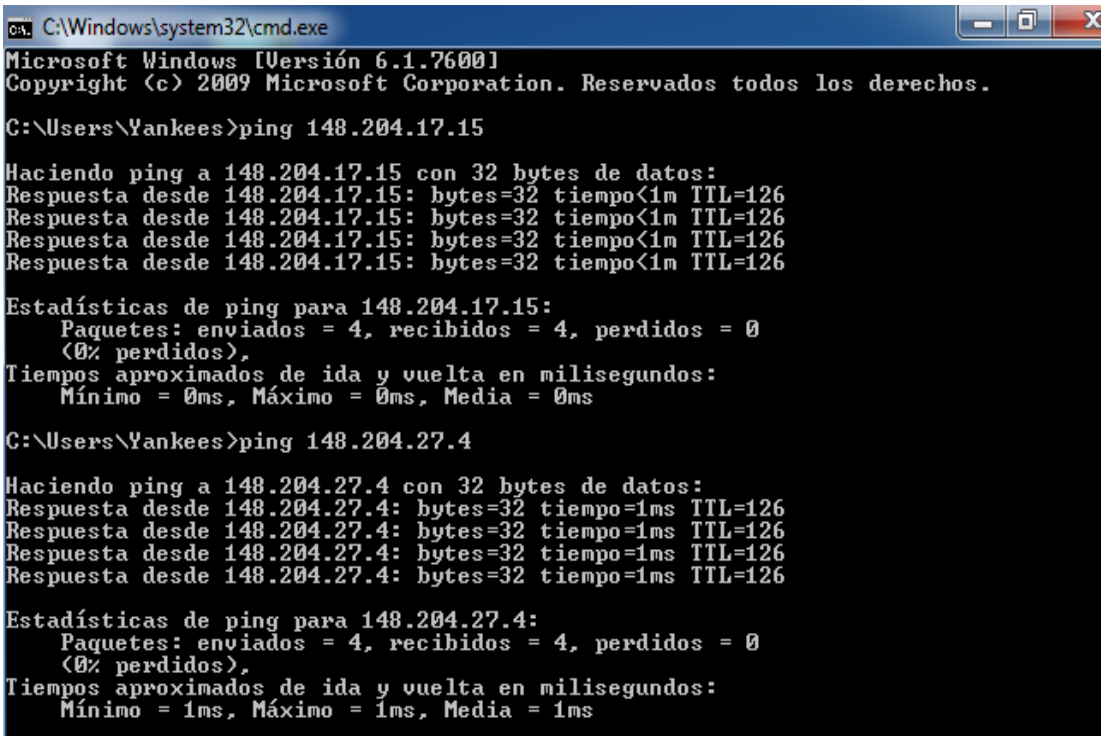


Figura 4.14.- Uso de la instrucción ping en direcciones IPv4

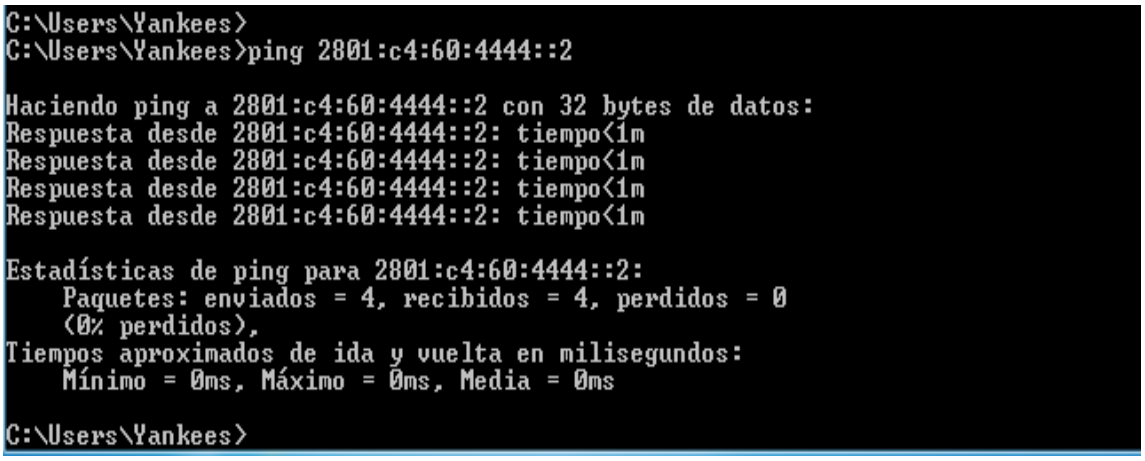


Figura 4.15.- Uso de la instrucción ping en direcciones IPv6

Una diferencia de IPv4 con respecto a IPv6 se observa que el campo de Tiempo de Vida, es renombrado en IPv6 como Límite de Saltos (Hop Limit), tiene una longitud de 8 bits (1 byte), su valor disminuye con cada nodo que reenvía el paquete, a esto se le conoce como salto, si este valor llega a 0 cuando el paquete IPv6 pasa por un enrutador, se rechaza y se envia un mensaje de error ICMPv6, esto se utiliza para que los datagramas no circulen indefinidamente por la red, tiene la misma función que el TTL en IPv4.

4.3.4.- Obtención de Métricas de enrutamiento

Para poder observar la Métrica de Enrutamiento, en las direcciones ya asignadas se utiliza la instrucción “tracert” la cual permite observar que ruta toman los paquetes para llegar a su destino con base a las direcciones IP asignadas.

```
C:\Users\ADMIN-CAPACITA>tracert 148.204.27.4

Traza a la dirección ROBERTO-PC [148.204.27.4]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  148.204.17.254
  2    <1 ms    <1 ms    <1 ms  148.204.10.1
  3     1 ms     1 ms     1 ms  148.204.27.4

Traza completa.

C:\Users\ADMIN-CAPACITA>tracert 148.204.30.1

Traza a la dirección YANKEES-PC [148.204.30.1]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  148.204.17.254
  2    <1 ms    <1 ms    <1 ms  148.204.15.2
  3    <1 ms    <1 ms    <1 ms  YANKEES-PC [148.204.30.1]

Traza completa.
```

Figura 4.16.- Uso de la instrucción tracert en direcciones IPv4

```
C:\Users\Roberto>tracert 2801:c4:60:6666::2

Traza a 2801:c4:60:6666::2 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  2801:c4:60:5555::1
  2     5 ms    <1 ms    <1 ms  2801:c4:60:2222::2
  3     5 ms     1 ms     1 ms  2801:c4:60:6666::2

Traza completa.
```

Figura 4.17.- Uso de la instrucción tracert en direcciones IPv6

Para poder comprender mejor las imágenes se observa que en cada una se tienen 3 métricas diferentes para IPv4 el cual está configurado con el Protocolo RIP se tienen 3 saltos para que los paquetes lleguen a su destino mientras que en IPv6 no son saltos son costos de enlace y al igual se tienen 3 costos para que los paquetes lleguen a su destino.

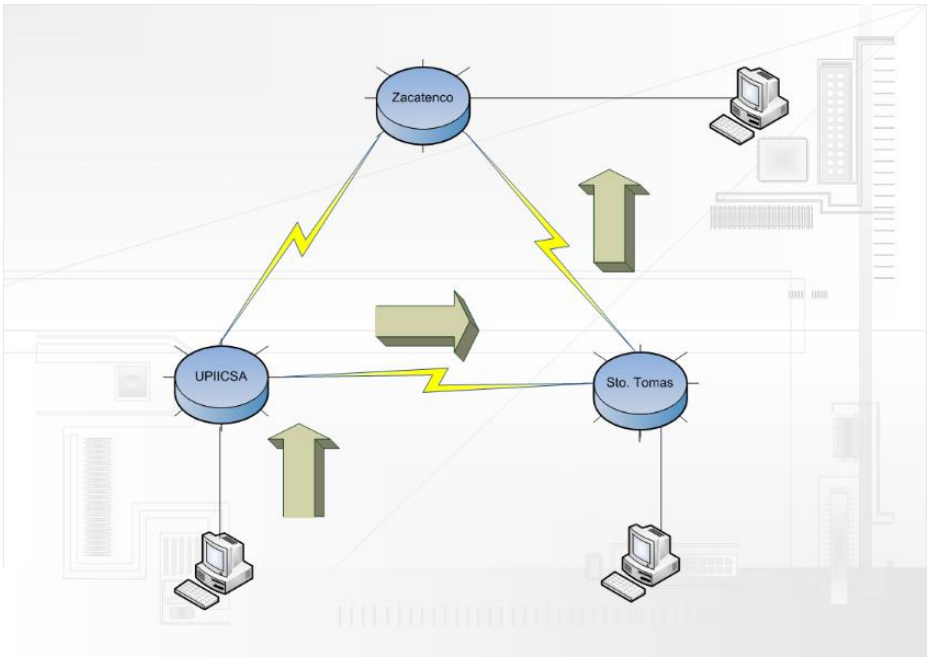


Figura 4.18.- Número de Saltos o Enlaces que se tienen en la Red

Una vez que se han hecho todas estas pruebas se procede a realizar las pruebas del método Doble Pila para comprobar dicho método se requiere que los nodos estén configurados con los protocolos IPv4 e IPv6 para poder mantener una comunicación como se observa en la siguiente figura:

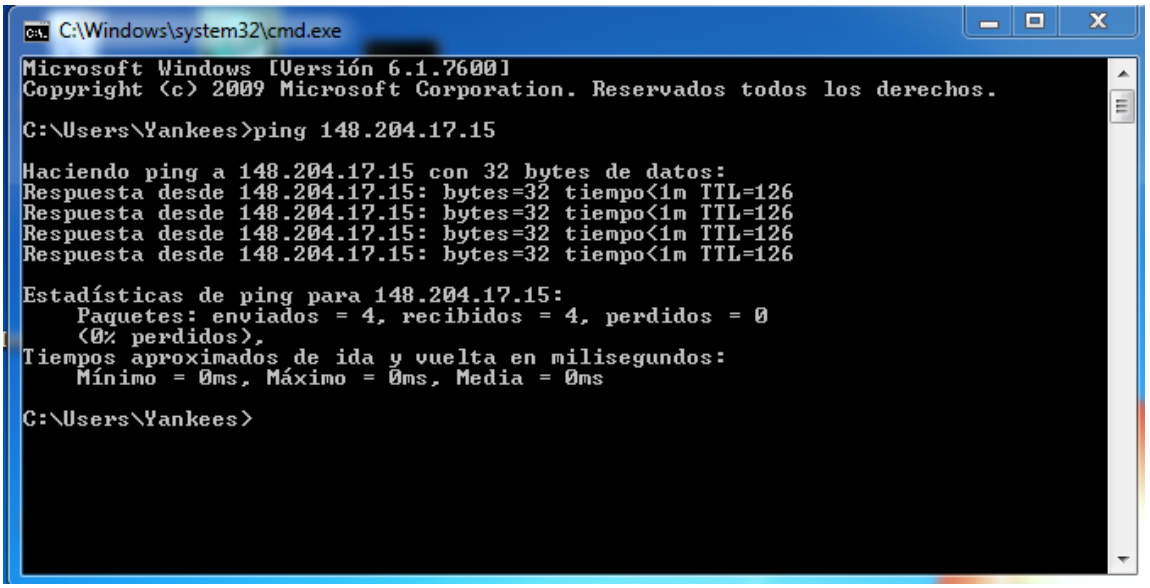


Figura 4.19.- PING a dirección IPv4

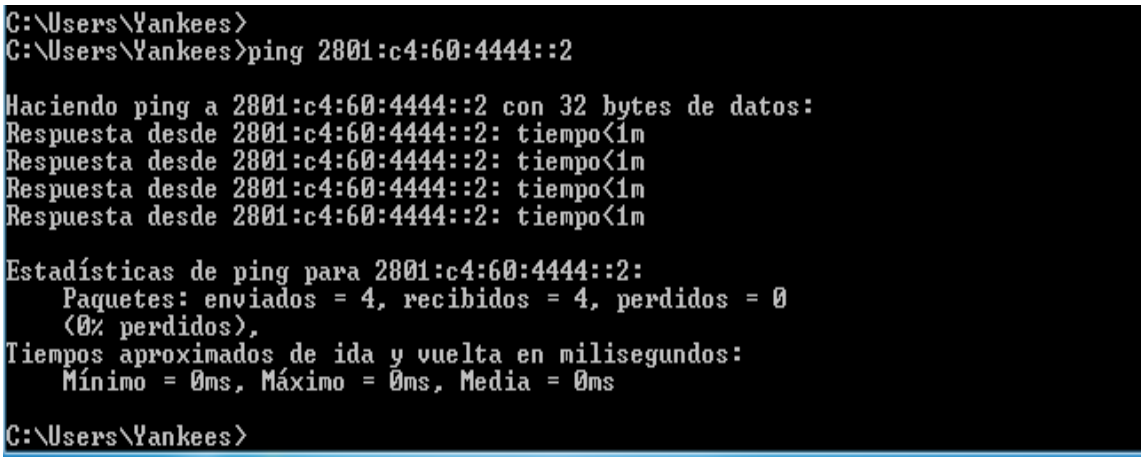


Figura 4.20.- PING a dirección IPv6

Para entender mejor el método doble pila, hay que entender la parte de la configuración de los nodos con ambos protocolos, pues es muy importante que estén configurados para que exista una conexión, al hacer PING como se muestra en las imágenes ya sea a una dirección IPv4 o IPv6 debe de establecer una comunicación, es decir que los paquetes de datos que fueron enviados sean los mismos que se reciban.

En la figura 4.14, se observa que al hacer un PING a una dirección IPv4 los paquetes que se envían son los mismos que llegan, claramente existe una comunicación, gracias a este protocolo se puede lograr que IPv6 se propague en la red sin ningún problema pues como los nodos de IPv4 tienen configurada una dirección IPv6, cuando se hace un PING a una dirección IPv6 se ayuda del protocolo IPv4 para poder mandar sus paquetes de datos y es aquí donde se puede apreciar el método doble pila pues gracias a que en un nodo de IPv4 se tienen configurados dichos protocolos uno se ayuda del otro para poder así tener una coexistencia entre ambos.

Por lo tanto, queda demostrado que el método doble pila es muy importante al hablar sobre una transición a este nuevo protocolo y es una gran manera de abrir nuevos caminos y empezar a pensar en un cambio el cual es importante a nivel mundial.

4.4.- Problemas

Uno de los problemas que se presentó durante la realización del proyecto fue con el programa “Packet Tracer”, el cual es una herramienta de aprendizaje y simulación de redes interactiva. Esta herramienta permite crear topologías de red, simular una red con múltiples representaciones visuales, etc.

El problema que se presentó con packet tracer al momento de querer habilitar el protocolo de enrutamiento OSPF en los nodos de IPv6 no existe una instrucción en el programa que propague de manera correcta OSPF en IPv6, es decir al querer mandar un PING los paquetes de datos no lograban pasar de la compuerta de enlace.

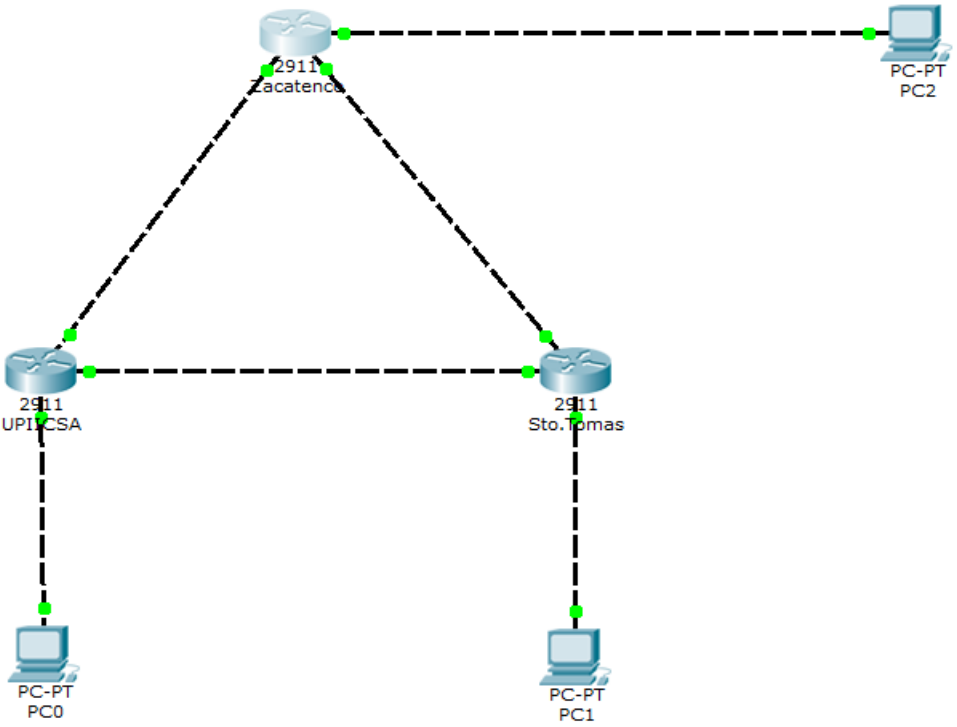


Figura 4.21.- Red Delta

Por tal motivo, se tuvo que interrumpir la simulación en dicho programa pues es vital que tanto IPv4 e IPv6 coexistan sin ningún problema, por lo tanto se tuvo que desarrollar parte de este proyecto utilizando enrutadores físicos los cuales no presentaron ningún problema.

Otro de los problemas que se presentó fue el cortafuegos y el antivirus, recordando que el cortafuegos comprueba la información procedente de Internet o de una red, y a continuación bloquea o permite el paso de esta al equipo.

Cuando se requiere mandar un ping de una máquina a otra y todo está bien configurado en el enrutador, se puede presentar el inconveniente de que no se reciba alguna respuesta del equipo destino y esto se debe a que el cortafuegos impide que se tenga una comunicación pues cree que la información que se está enviando no es segura ya que al ocupar la instrucción ping se abren puertos importantes, así que se necesita deshabilitar el cortafuegos para poder tener una comunicación.

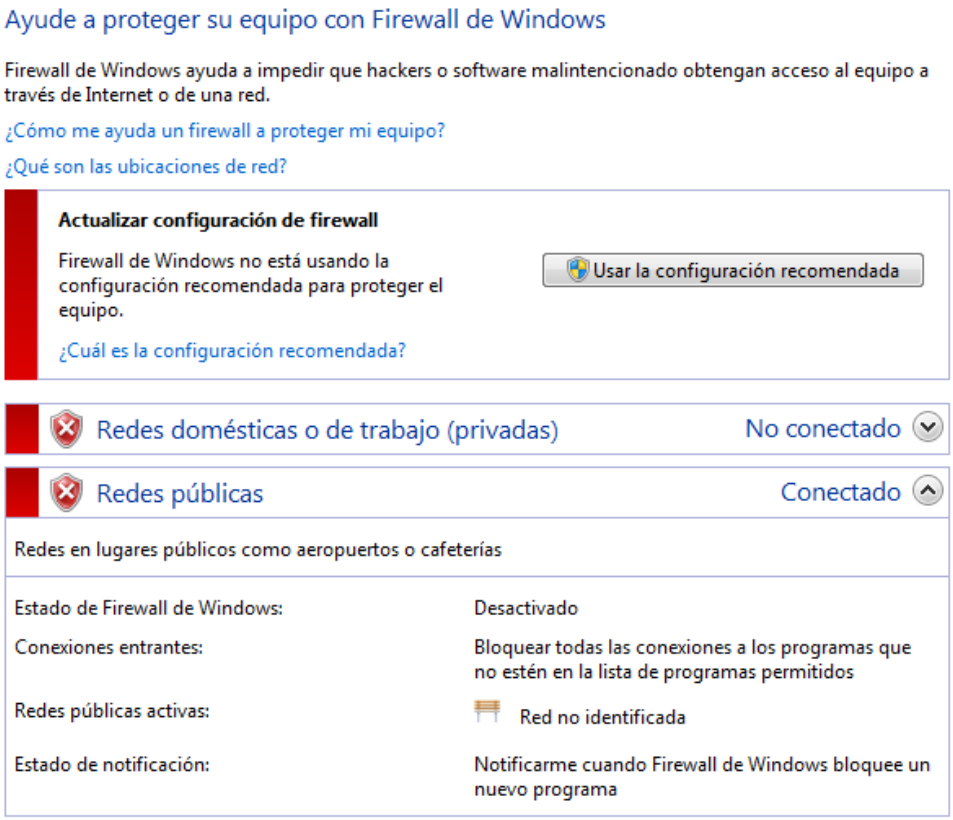
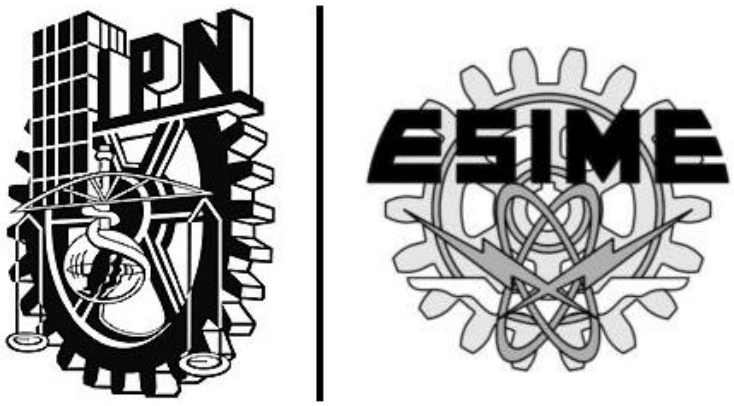


Figura 4.22.- Deshabilitación del cortafuegos del ordenador

Por otra parte, el problema con el Antivirus puede ser similar al que se experimenta con el cortafuegos, por lo que hay que desactivarlos para hacer las pruebas de ping correctamente, es recomendable mencionar que no todos los antivirus hay que deshabilitarlos pues depende de este si lo bloquea o no el PING que se manda.



Conclusiones

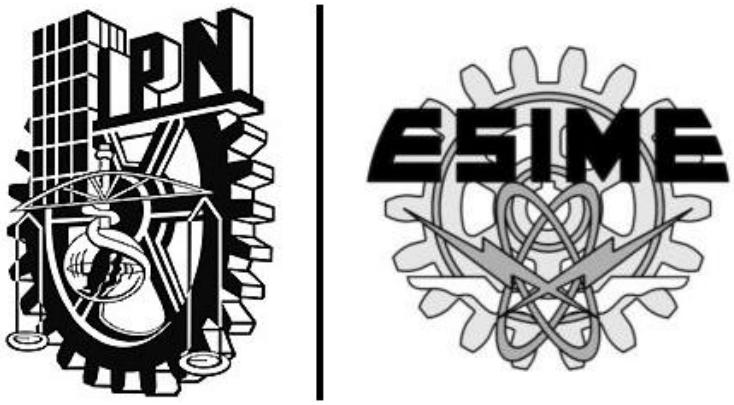
Conclusiones

El problema del agotamiento de las direcciones en IPv4 da pie a la búsqueda de un mecanismo de transición hacia su siguiente versión IPv6; al encontrar una coexistencia entre ambos Protocolos de Internet pueden surgir algunas complicaciones, pero con la aplicación de algunos métodos existentes es posible y de manera más sencilla realizar una transición.

Cabe mencionar, que el método más sencillo para realizar una transición entre ambos protocolos es el de doble pila, de esta forma se permitirá el acceso tanto aplicaciones de IPv4 como IPv6, así que queda comprobado que el método doble pila puede ser una solución para que no exista un agotamiento de direcciones IPv4.

Por otro lado, el cuestionar cuanto tiempo tardará una coexistencia de IPv4 e IPv6 implementado en organizaciones, escuelas, oficinas, casas etc., depende de que tan bien, esté preparada cada una de ellas para dar el salto a la siguiente generación del protocolo e implementar un mecanismo de transición.

Por último, es necesario considerar que por razones de tiempo y de disponibilidad sea un proceso largo y exclusivo en el cual, no todos los usuarios actuales de IPv4 podrían beneficiarse a corto plazo de las ventajas que ofrece IPv6, pero sí se puede decir que el hecho de que la transición está en proceso es un gran avance para el desarrollo y desempeño global a futuro.



Bibliografía / Referencia

Bibliografía

[1] STALLINGS, William. Comunicaciones y Redes de Computadoras, 7ª ed. Pearson Education, 2004, 896p, ISBN: 9788420541105.

[2] STALLINGS, William, Comunicación y Redes de Computadoras, 6ª ed. Pearson Education, 2004, ISBN: 85-205- 4110-9.

[3] COMER Douglas, Redes globales de información con Internet y TCP/IP, ed. Prentice-Hall, EUA, 3 ª edición.

[4] ROBLEDO Cornelio, Redes de Computadoras, México D.F., ed. IPN, 2002.

[5] TANENBAUM Andrew, Redes de Computadoras, 4ª ed., Prentice-Hall, México 2003, ISBN: 970-26-0162-2.

[6] MILLAN Ramón, Redes de datos y convergencia IP, 1ª ed., Alfa omega grupo editor, 2006.

[7] KUROSE James & ROSS Keith, Redes de computadoras un enfoque descendente, ed. Pearson Educación, 2010.

[8] MALONE, IPv6 Network Administration, Editorial 0`Reilly, 2005.

[9] ESPAÑA Carmen, Servicios avanzados de telecomunicaciones, ed. Díaz de Santos, 2008.

[10] HILL Brian, Manual de Referencia Cisco, ed. Mc Graw Hill/Interamericana de España, 2002, ISBN: 968-880-541-6.

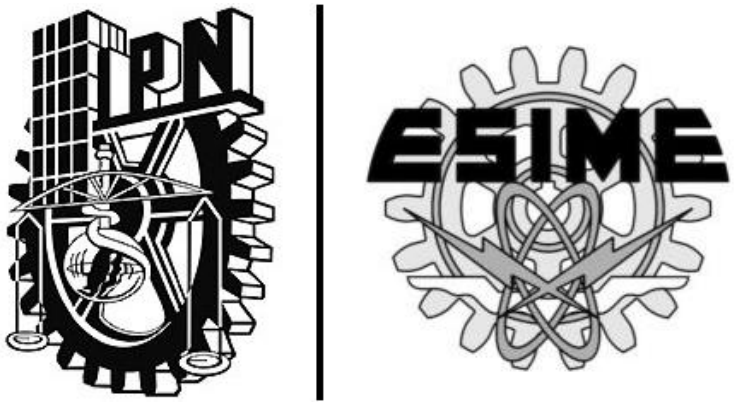
[11] MAYERS Mike, Redes Administración y mantenimiento, ed. Anaya Multimedia, 2010.

[12] CCNA 1 y 2: Conceptos básicos sobre networking, 3ª ed., Pearson Education, 2004, 1016p, ISBN: 9788420540795.

[13] CCNA Exploration: Conceptos y protocolos de enrutamiento, Pearson Education, 2004.

[14] MOY John, OSPF Anatomy of an Internet Routing Protocol, Addison-Wesley, 1998. 340p, ISBN: 0201634724.

[15] NOVO Alejandro, LOPEZ Ángel, Protocolos de Internet diseños e implementación en sistemas UNIX, RA-MA, 1999, 400p, ISBN: 9788478973828.



Acrónimos

Acrónimos

ARPANET: Advanced Research Projects Agency Network / Agencia de investigación de proyectos avanzados de redes de computadoras.

DARPA: Defense Advanced Research Projects Agency / Agencia de Proyectos de Investigacion Avanzados de Defensa.

DHCP: Dynamic Host Configuration Protocol / Protocolo de Configuración Dinámica de Host.

DNS: Domain Name System / Sistema de Nombres de Dominio.

FTP: File Transfer Protocol / Protocolo de Transferencia de Archivos.

HTTP: Hypertext Transfer Protocol / Protocolo de Transferencia de Hypertexto.

IP: Internet Protocol / Protocolo de Internet.

LAN: Local Area Network / Red de Área Local.

OSI: Open Systems Interconnection / Modelo de Interconexión de Sistemas Abiertos.

PDU: Protocol Data Unit / Unidad de Datos de Protocolo.

SMTP: Simple Mail Transfer Protocol / Protocolo de Transferencia Simple de Correo Electrónico.

SNMP: Simple Network Management Protocol / Protocolo Simple de Administración de Red.

TCP: Transmission Control Protocol / Protocolo de Control de Transmisión.

TELNET: Telecommunications Network.

WAN: Wide Area Network / Red de Area.

CIDR: Classless Inter-Domain Routing / Enrutamiento entre dominios sin clases.

IETF: Internet Engenieering Task Force / Grupo de Trabajo de Ingeniería de Internet.

IHL: Internet Header Length / Longitud cabecera internet.

IPng: Internet Protocol Next Generation / Protocolo de Internet Siguiente Generación.

IPTV: Internet Protocol Television / Protocolo de Internet para Televisión.

MTU: Maximum Transmission Unit / Unidad Máxima de transferencia.

NAT: Network Address Translation / Traductor de Direcciones de Red.

PPP: Point to Point Protocol / Protocolo Punto a Punto.

QoS: Quality of Service / Calidad del Servicio.

RFC: Request for Comments / Solicitud de Comentarios.

TTL: Time to Live / Tiempo de vida.

VLSM: Variable Length Subnet Mask / Mascara de Subred de Longitud Variable.

Mbps: Mega bit por segundo.

RIP: Routing Information Protocol / Protocolo de Información de Enrutamiento.

IGRP: Interior Gateway Routing Protocol / Protocolo de Enrutamiento de Compuerta de Enlace Interior.

EIGRP: Enhanced Interior Gateway Routing Protocol / Protocolo de enrutamiento de Compuerta de Enlace Interior Mejorado.

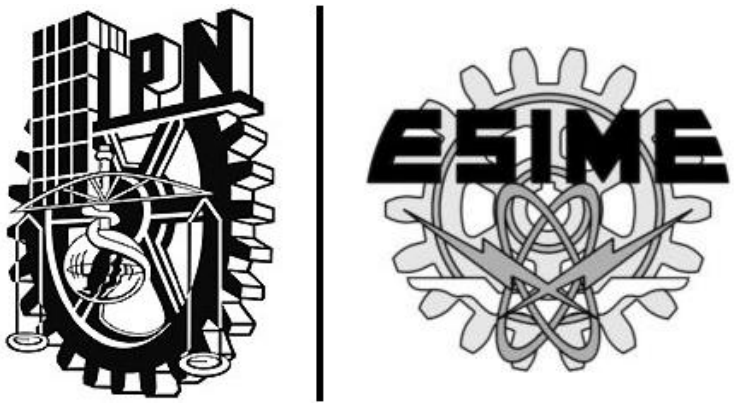
IS- IS: Protocolo de estado de enlace.

OSPF: Open Shortest Path First / El Camino más Corto Primero.

eBGP: External Border Gateway Protocol / Protocolo de Compuerta de Enlace FronterizoExterior.

iBGP: Internal Border Gateway Protocol / Protocolo de Compuerta de Enlace Fronterizo Interno.

IPX: Internetwork Packet Exchange / Intercambio de Paquetes Inter-red.



Apéndice

Wireshark

Una herramienta básica para observar los mensajes intercambiados entre aplicaciones es un analizador de protocolos (mejor conocido en inglés como “packet sniffer”). Un analizador de protocolos es un elemento pasivo, únicamente observa mensajes que son transmitidos y recibidos desde y hacia un elemento de la red, pero nunca envía el mismo mensaje. En su lugar, un analizador de protocolos recibe una copia de los mensajes que están siendo recibidos o enviados en el terminal donde está ejecutándose.

Está compuesto principalmente de dos elementos: una librería de captura de paquetes, que recibe una copia de cada trama de enlace de datos que se envía o recibe, y un analizador de paquetes, que muestra los campos correspondientes a cada uno de los paquetes capturados. Para realizar esto, el analizador de paquetes ha de conocer los protocolos que está analizando de manera que la información mostrada sea coherente.

Wireshark se trata de un programa gratuito disponible para varias plataformas (Unix, Windows y Mac OS). Se puede descargar desde www.wireshark.org., donde además, existe documentación asociada y un manual de usuario.

Una vez instalado el programa se procede a realizar la captura de paquetes para comprobar que los protocolos usados por IPv6 tienen una ejecución durante el método de doble pila.

Figura A.- Pantalla de Inicio de Wireshark

Ya inicializado el programa se realiza un PING desde el símbolo de sistema para que empiece la captura de paquetes.

```
C:\Users\Yankees>
C:\Users\Yankees>
C:\Users\Yankees>ping 2801:c4:60:5555::2

Haciendo ping a 2801:c4:60:5555::2 con 32 bytes de datos:
Respuesta desde 2801:c4:60:5555::2: tiempo=2ms
Respuesta desde 2801:c4:60:5555::2: tiempo=1ms
Respuesta desde 2801:c4:60:5555::2: tiempo=1ms
Respuesta desde 2801:c4:60:5555::2: tiempo=1ms

Estadísticas de ping para 2801:c4:60:5555::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Yankees>_
```

Figura B.- PING al ordenador desde el símbolo de sistema

Una vez hecho esto se inicia el programa de nuevo para empezar a apreciar la captura de los paquetes tanto de IPv4 como de IPv6.

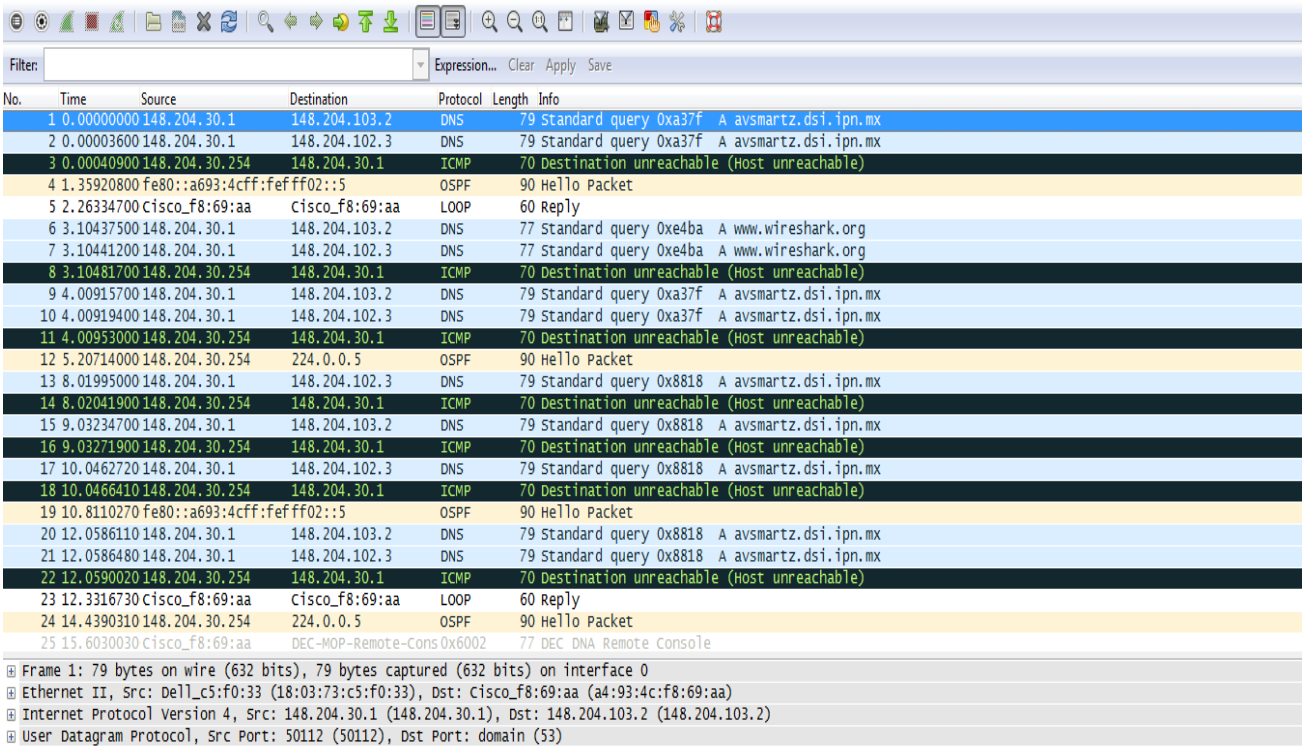


Figura C.- Captura de protocolos IPv4 en WireShark

En la anterior imagen, se puede observar la captura de protocolos en IPv4 y así se pueden apreciar las direcciones a las cuales fue aplicada la instrucción PING, capturando protocolos como DNS, ICMP, OSPF.

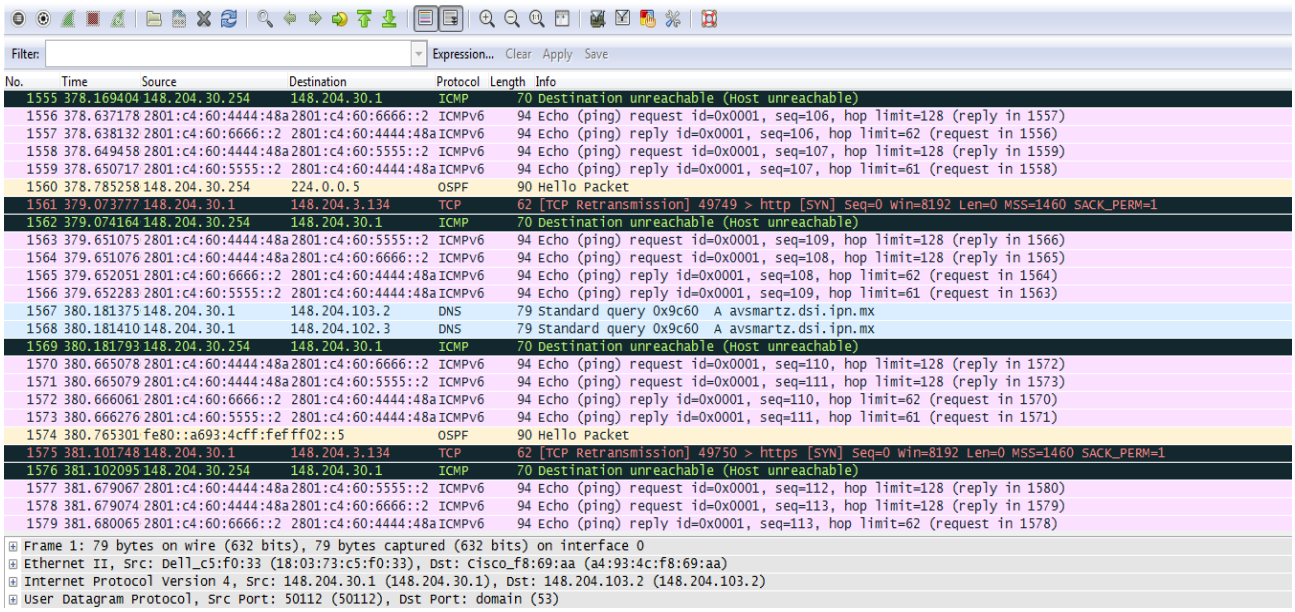


Figura D.-Captura de Protocolos IPv6 en Wireshark

Como se ve en la imagen las direcciones IPv6 configuradas en los ordenadores a las cuales se realizó un PING contienen una serie de protocolos que cambian a comparación de IPv4 el más simbólico es el ICMPv6 pues es un protocolo único de IPv6 pero que gracias a la ayuda de IPv4 se puede propagar cuando envía sus paquetes de datos, existen otros protocolos como OSPF, TCP, DNS, etc.; que le permiten al protocolo IPv6 ocupar las aplicaciones de IPv4.

Código de Configuración de los Enrutadores

Código Zacatenco

```
! Last configuration change at 22:21:40 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:46:58 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:46:58 UTC Fri Feb 28 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
computadoraname Zacatenco
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
license udi pid CISCO2911/K9 sn FTX1628A04W
!
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 148.204.5.1 255.255.255.0
 duplex auto
```

```
 speed auto
 ipv6 address 2801:C4:60:1111::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 148.204.15.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:3333::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/2
 ip address 148.204.30.254 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:4444::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
enrutador ospf 1
 network 148.204.5.0 0.0.0.255 area 0
 network 148.204.15.0 0.0.0.255 area 0
 network 148.204.30.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 enrutador ospf 1
 enrutador-id 1.1.1.1
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
```

Código UPIICSA

```
! Last configuration change at 22:29:56 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:48:01 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:48:01 UTC Fri Feb 28 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
computadoraname UPIICSA
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO2911/K9 sn FTX1629AJ7V
!
!
redundancy
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 148.204.10.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:2222::1/64
 ipv6 enable
```

```
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 148.204.5.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:1111::2/64
 ipv6 enable
!
interface GigabitEthernet0/2
 ip address 148.204.27.254 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:5555::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
enrutador ospf 1
 network 148.204.5.0 0.0.0.255 area 0
 network 148.204.10.0 0.0.0.255 area 0
 network 148.204.27.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ipv6 enrutador ospf 1
 enrutador-id 3.3.3.3
!
!
control-plane
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

Código Santo Tomas

```
! Last configuration change at 22:27:47 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:48:13 UTC Fri Feb 28 2014
! NVRAM config last updated at 22:48:13 UTC Fri Feb 28 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
computadoraname StoTomas
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO2911/K9 sn FTX1629ALQ4
!
!
redundancy
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 148.204.15.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:3333::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

```
interface GigabitEthernet0/1
 ip address 148.204.10.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:2222::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/2
 ip address 148.204.17.254 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2801:C4:60:6666::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
enrutador ospf 1
 network 148.204.10.0 0.0.0.255 area 0
 network 148.204.15.0 0.0.0.255 area 0
 network 148.204.17.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ipv6 enrutador ospf 1
 enrutador-id 2.2.2.2
!
!
control-plane
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```