Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO

Sergio Javier Girón de Paz

Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, febrero de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

SERGIO JAVIER GIRÓN DE PAZ
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, FEBRERO DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Francisco Javier González López
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 30 de agosto de 2012.

Sergio Javier Girón de Paz

Guatemala 25 de Agosto de 2014

Ingeniero
Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Estimado Ingeniero Guzmán.

Me permito dar aprobación al trabajo de graduación titulado: **PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO**, del señor **Sergio Javier Girón de Paz**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 47. 2014
Guatemala, 4 de AGOSTO 2014.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO, del estudiante Sergio Javier Girón de Paz, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

STO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 47. 2014.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; SERGIO JAVIER GIRÓN DE PAZ titulado: PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 1 DE OCTUBRE 2,014.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 058 .2015

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO,** presentado por el estudiante universitario: **Sergio Javier Girón de Paz,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 16 de febrero de 2015

/gdech

ACTO QUE DEDICO A:

Dios	Por ser una importante influencia en mi carrera, entre otras cosas.
Mis padres	José Pérez y Rosa López de Pérez. Su amor será siempre mi inspiración.
Mi esposa	Lucía Díaz de Pérez. Por ser una importante influencia en mi carrera, entre otras cosas.
Mis hijos	José y Lucía. Por ser dos ángeles a mi vida.
Mis tíos	Mario Pérez, Carmen Pérez. Por ser una importante influencia en mi carrera, entre otras cosas.
Señor 4	Por ser una importante influencia en mi carrera, entre otras cosas.
Señor 5	Por estar ahí…
Señorita 1	Por estar ahí…
Señorita 2	Por estar ahí…
Señorita 3	Por estar ahí…

Señorita 4	Por estar ahí…
¡¡¡OJO!!!	Si no llega a 2 páginas dejar esta en blanco.
Etc…	Etc..

AGRADECIMIENTOS A:

La Universidad de San Carlos de Guatemala	Por ser una importante influencia en mi carrera, entre otras cosas.
Facultad de Ingeniería	Por ser una importante influencia en mi carrera, entre otras cosas.
Mis amigos de la Facultad	José Pérez, María Díaz, Clara Domínguez, etc.
Señor 2	Por ser una importante influencia en mi carrera, entre otras cosas.
Señor 3	Por ser una importante influencia en mi carrera, entre otras cosas.
Señor 4	Por ser una importante influencia en mi carrera, entre otras cosas.
Señor 5	Por estar ahí…
Señorita 1	Por estar ahí…
Señorita 2	Por estar ahí…
Señorita 3	Por estar ahí…

Señorita 4	Por estar ahí…
Etc…	Etc..

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Nal	Capa de acceso a la red

GLOSARIO

AS	Autonomous System, Sistema autónomo.
BROADCAST	Forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.
CRC	Cyclic Redundancy Check, Comprobación de Redundancia Cíclica.
DHCP	Dynamic Host Configuration Protocol, Protocolo de Configuración de Host Dinámico.
DNS	Domain Name System, Sistema de Nombres de Dominio.
E2E	End to End, Extremo a Extremo.
ETHERNET	Estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD).
HSRP	Hot Stand-by Router Protocol, Protocolo de Redundancia de Gateway.

IANA	Internet Assigned Numbers Authority, Autoridad de Números Asignados de Internet.
ICMP	Internet Group Management Protocol, Protocol de Internet para manejo de grupos.
IEEE	Institute of Electrical and Electronics Engineers, Instituto de Ingeniería Eléctrica y Electrónica.
IETF	Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet.
IGP	Interior Gateway Protocol, Protocolo de Salidas Internas.
IP-IS	Protocolo de estado de enlace.
IPV4	Internet Protocol Version 4, Protocolo de Internet Versión 4.
IPV6	Internet Protocol Version 6, Protocolo de Internet Versión 6.
ISP	Internet Service Provider, Proveedor de Servicios de Internet.
LAN	Local Area Network, Redes de Área Local.

RESUMEN

En el trabajo de graduación se presentan las técnicas de transición de IPv4 a IPv6 que existen en la actualidad. Se proponen los túneles como la mejor técnica de transición de IPv4 a IPv6 para redes de datos de proveedores de servicio.

En el capítulo I se dan a conocer todos los fundamentos básicos de introducción a las redes de datos de proveedores de servicio tocando temas como el modelo OSI, el modelo TCP/IP, los fundamentos de WAN y los fundamentos de LAN.

En el capítulo II se explican los fundamentos básicos del protocolo IP en redes datos de proveedores de servicio, donde se exponen los detalles de las cabeceras de los paquetes IPv4 e IPv6, así como temas de enrutamiento y direccionamiento IPv4 e IPv6.

En el capítulo III se presentan las técnicas de transición de IPv4 a IPv6 en redes de datos de proveedores de servicio que existen actualmente:

- Doble pila
- Técnicas basadas en túneles IPv4 - IPv6
- Técnicas basadas en traductores IPv6 <-> IPv4

En el capítulo IV se hace un análisis de los túneles IPv4 – IPv6 como técnica de transición de IPv4 a IPv6, exponiendo sus ventajas y desventajas para una red de datos de proveedores de servicio.

OBJETIVOS

General

Elaborar una propuesta técnica de la utilización de túneles como procedimiento de transición de IPv4 a IPv6 en redes de datos de proveedores de servicio.

Específicos

1. Dar a conocer los fundamentos básicos de introducción de redes de datos de proveedores de servicio.

2. Presentar los fundamentos básicos del protocolo IPv4 e IPv6 en redes de datos de proveedores de servicio.

3. Dar a conocer las distintas técnicas de transición de IPv4 a IPv6 que existen en la actualidad para redes de datos de proveedores de servicio.

4. Proponer la técnica de túneles como la mejor opción de transición de IPv4 a IPv6 para redes de datos de proveedores de servicio.

INTRODUCCIÓN

Las redes de datos de los proveedores de servicio pueden ser mapeadas en siete categorías si se sigue el modelo OSI, o cuatro si se sigue el modelo TCP/IP.

Independientemente del tipo de modelo que se siga, en ambos existe el protocolo IP que se encarga de todo el direccionamiento y enrutamiento de paquetes dentro de las redes de datos. Actualmente se trabaja sobre la versión 4 del protocolo IP (IPv4), sin embargo, las direcciones que permite manejar dicha versión se están acabando a nivel global y el implementar la nueva versión del protocolo (IPv6) es inevitable.

Esto trae consigo la necesidad que exista una coexistencia entre IPv4 e IPv6, ya que aunque en su tiempo IPv6 reemplazará por completo a IPv4, la transición será más lenta. Los administradores como los operadores de las redes actualmente se cuestionan: ¿Qué hacer durante este período de transición, para seguir ofreciendo los servicios que ya brinda por redes IPv4 e iniciar servicios IPv6 sin que una limite a la otra?

En el mercado existen 3 técnicas de transición: Dual Stack, Traductores y túneles, es esta última, sobre la cual este trabajo de graduación hace un análisis de lo que implica su implementación, tomando solo los factores técnicos de diseño, control y operación a manera que puedan tener una visibilidad completa de lo que se viene y más importante aún, ¿qué pueden iniciar a hacer desde ya, para que esa transición sea lo más transparente posible?

.

1. INTRODUCCIÓN A FUNDAMENTOS DE RED

Se entiende por red a la interconexión entre dos equipos terminales o más, con el propósito básico de compartir información y recursos.

Para que este propósito se pueda llevar a cabo, primordialmente se necesita de algún medio de comunicación (canal de comunicación), el cual dependiendo de las necesidades puede variar desde un cable coaxial hasta fibra óptica y todos los medios de comunicación que entre ellos se encuentran.

Una vez definido el medio de comunicación por el cual los equipos terminales compartirán información y recursos, se debe explicar una serie de protocolos de comunicación, los cuales son necesarios para que todos los equipos terminales que constituyen una misma red hablen el mismo idioma.

El hecho que distintos equipos terminales deban cumplir con ciertos protocolos de comunicación, hace que nazca la necesidad de crear modelos de red para que exista una forma estándar de nombrar e identificar las partes de la red.

1.1. Modelos TCP/IP y OSI

El término modelo de red se refiere a un conjunto organizado de documentos. Estos documentos individualmente pueden definir un protocolo, que no es más que un conjunto de reglas lógicas que los equipos deben de seguir para poder comunicarse. Otros documentos, por ejemplo, pueden definir los niveles de voltaje y corriente utilizados en algún cable de interconexión.

Colectivamente, estos documentos definen todos los detalles de cómo se debe crear una red.

En su momento, se pensó en crear un modelo de red estándar, para que se pudieran comunicar equipos de distintas marcas entre sí de una manera simple, siempre que se cumplieran con las reglas y protocolos descritos por dicho modelo. Dos fueron los modelos estándar propuestos: el modelo OSI (Sistema Abierto de Interconexión) propuesto por la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés) alrededor de 1970.

Una segunda propuesta, nace de los trabajos del ARPA (Advanced Research Proyect Agency) del Departamento de Defensa de los Estados Unidos, durante 1960 y 1970. Esta propuesta fue trabajada tanto a través de universidades como por medio de centros de investigación.

Al final, la propuesta ganadora fue TCP/IP, sin embargo, hoy en día se sigue haciendo referencia al modelo OSI por la manera en que ellos definen sus categorías o capas dentro del modelo, a manera que uno podría tomar cualquier red y separarla en categorías, niveles o capas según las definiciones y conjunto de protocolos y reglas establecidas por OSI.

También existe cierta similitud entre el modelo OSI y el modelo TCP/IP, por lo que sigue siendo muy útil aprender tanto un modelo como el otro, aunque en la práctica, el que se utilice sea el modelo TCP/IP.

1.1.1. Modelos TCP/IP

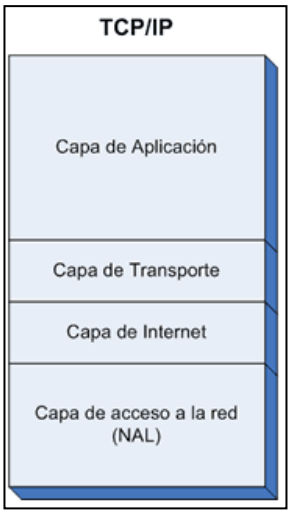
El modelo TCP/IP define una colección extensa de protocolos que permite a los equipos terminales comunicarse. Al igual que cualquier modelo de red o

arquitectura de red, TCP/IP clasifica estos distintos protocolos en distintas categorías o capas.

Este modelo, diseño en principio para enrutamiento, tiene un grado muy elevado de fiabilidad, es utilizado desde campos universitarios, complejos empresariales hasta teléfonos celulares y en domótica.

Uno de los inconvenientes que presenta este modelo es que tiende a ser más lento en redes con volumen de tráfico bajo, aunque para volúmenes de tráfico grande es muy eficiente y suele ser más complejo de configurar que otros modelos como netBEUI o IPX/SPX.

Figura 1. **Modelo TCP/IP**



Fuente: elaboración propia.

La capa de aplicación es un conjunto de protocolos que brindan los servicios a las aplicaciones que se estén ejecutando en los equipos terminales. Es importante aclarar en este punto, que esta capa, más que definir la

aplicación que se está ejecutando, define los servicios que la aplicación necesita. Dicho en otras palabras, el usuario final no interactúa en ningún momento de manera directa con la capa de aplicación. Por ejemplo, un usuario que está utilizando algún programa para chatear no se ve en la necesidad de codificar la información y los datos del destinatario, para luego entregarla a la siguiente capa de transporte para que se realice el envío.

La capa de transporte, más que una capa adicional del modelo TPC/IP, es el corazón de todos los protocolos de redes. Es esta capa la encargada de llevar a cabo el control de la transmisión y la gestión de errores. Tiene como objetivo principal proporcionar servicios confiables y eficientes, encargándose de la recuperación de eventos como paquetes perdidos o mal formados. Es gracias a esta capa que los programadores de aplicaciones pueden escribir código, según un conjunto estándar de primitivas y hacer que esas aplicaciones funcionen en una amplia variedad de redes. Son dos los protocolos que se encuentran en esta capa: TCP y UDP. UDP es un protocolo no orientado a conexión. Es decir, cuando un equipo terminal A envía información a un equipo terminal B el flujo es unidireccional.

No se crea ningún tipo de sesión previa entre equipos terminales antes de realizar la transferencia de datos. El equipo terminal B no envía ningún tipo de confirmación al emisor. Contrariamente a UDP, TCP es un protocolo orientado a conexión. En este caso, el equipo terminal B es previamente notificado de la transferencia de datos y luego de la transferencia confirma la correcta llegada de los datos.

En este punto interviene el control CRC, la cual es una ecuación matemática que permite verificar la integridad de los datos transmitidos. De esta manera, en caso que los datos recibidos sean erróneos, el protocolo TCP

permite que los equipos terminales receptores soliciten al emisor la retransmisión de los datos corruptos.

La capa de internet, definida en su gran mayoría por el protocolo de internet (IP), define los datagramas y administra las nociones de direcciones IP. Es aquí donde se permite el enrutamiento de datagramas (paquetes de datos) a equipos terminales remotos junto con la administración de su división y ensamblaje cuando se reciben.

Son 5 los protocolos empleados en esta capa: IP, ARP, ICMP, RARP e IGMP siendo los primeros tres los más importantes.

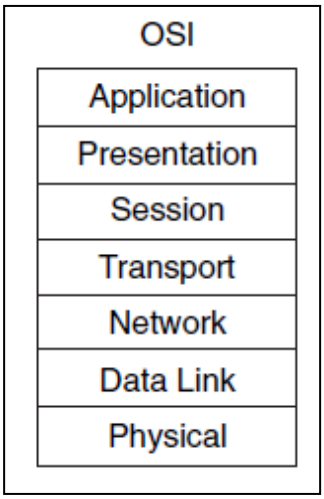
La capa de acceso a la red es conformada por un conjunto de protocolos que definen todo lo referente con el medio físico, al cual un equipo terminal se debe conectar para poder transmitir datos a través de cualquier red. Esta capa contiene un gran número de protocolos, entre los que se pueden mencionar todas las variaciones del protocolo Ethernet y otros estándares de LAN (redes de área local). Esta capa también incluye los protocolos referentes a WAN (redes de área amplia), entre los que se encuentran PPP y Frame Relay entre otros. Se definen el tipo de conectores, cableado y niveles de voltaje necesarios para poder transmitir información a través de una LAN o una MAN.

En cada nivel, el paquete de datos cambia su forma o aspecto. Por lo tanto las designaciones del mismo cambian según las capas. El paquete de datos se denomina mensaje en la capa de aplicación. El mensaje luego es encapsulado en forma de segmento en la capa de transporte. En la capa de internet, el segmento es encapsulado nuevamente y recibe el nombre de datagrama. Finalmente, en la capa de acceso a la red se encapsula el datagrama y se habla entonces de una trama.

1.1.2. El modelo OSI

OSI, derivado de sus siglas en inglés (Open System Interconnection), define siete capas, siendo cada una de estas un conjunto de funciones y protocolos de red. Es importante decir que al igual que el modelo TCP/IP, en su mayoría más que crear protocolos nuevos, hicieron referencia a protocolos ya existentes y los fueron agrupando en las distintas capas que cada modelo define. Un ejemplo de esto podría ser el protocolo Ethernet definido por la IEEE, OSI en vez de crear un nuevo Ethernet simplemente hace referencia en la capa dos de su modelo al protocolo ya definido por la IEEE.

Figura 2. **El modelo OSI**



Fuente: elaboración propia.

De las siete capas definidas por el modelo OSI se puede hacer una división, tomando las capas de la siete a las cinco (aplicación, presentación y sesión) como capas cuyas funciones se centran básicamente en la aplicación como tal y las capas de la cuatro a la uno (transporte, red, enlace de datos y

físico) como capas cuyas funciones se centrar en la entrega de información entre equipos terminales.

La capa de aplicación provee una interfaz entre el software de comunicación y cualquier aplicación que necesite comunicarse fuera del equipo terminal, es decir, con otro equipo terminal ya sea conectado directamente o indirectamente a este. Es en esta también se definen procesos para autenticación.

La capa de sesión, contiene protocolos que permiten que la comunicación entre distintas aplicaciones en distintos equipos terminales sea transparente para las aplicaciones. Esta capa se ocupa de tres funciones principales que son: formateo de datos, cifrado y compresión de datos.

Como formateo de datos se pueden mencionar 2 formatos de texto: ASCII y EBCDIC. Ambos formatos contienen caracteres simples y carecen de comandos de formato sofisticados. La diferencia principal entre los dos códigos es que ASCII se utiliza en computadoras mientras EBCDIC se utiliza principalmente en sistemas mainframe. La capa de presentación aquí funciona como un traductor. Asimismo, esta capa se encarga del cifrado de información durante una transmisión para poder proteger información confidencial que se envía a través de internet, como por ejemplo, las transacciones financieras.

La capa de presentación también se ocupa de la compresión de archivos. La compresión funciona mediante el uso de algoritmos para reducir el tamaño de archivos, este busca patrones de bit repetidos en el archivo y entonces los reemplaza con un token. Un token es un patrón de bit muchas veces más corto que representa el patrón largo.

La capa de sesión permite a los usuarios de diferentes máquinas de una red establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, aunque esta capa se diferencia de la capa de transporte por los servicios que proporciona. Entre los servicios proporcionados por la capa de sesión están: intercambio de datos, administración del dialogo, sincronización, administración de actividades y notificación de excepciones.

La capa de transporte, brinda servicios para garantizar el envío íntegro de la información entre equipos terminales. Entre las funciones que se encuentran se pueden mencionar: multiplexación utilizando puertos, corrección de errores, control de flujo de datos, inicio y finalización de conexiones y ordenamiento de segmentos de datos. A diferencia de otras capas, en ésta capa están definidos dos protocolos nada más: TCP y UDP. TCP es un protocolo orientado a conexión mientras UDP no lo es.

La capa de red define tres funciones principales: direccionamiento lógico, ruteo y determinación de rutas. El concepto de ruteo se define como la capacidad de los enrutadores de enviar tráfico hacia su destino final. El direccionamiento lógico indica que cada equipo o dispositivo pueden ser utilizados por el proceso de ruteo. La determinación de la ruta indica la mejor ruta hacia un destino de las varias rutas que se pudieran presentar a ese mismo destino (de presentarse varias rutas).

La capa de enlace de datos define las reglas y protocolos que determinan cuando un dispositivo dado puede o no enviar información sobre un medio. Se definen encabezados y colas para garantizar el envío de datos entre los dos dispositivos. Es en la cola donde se define el chequeo de secuencia de la trama, FCS por sus siglas en inglés, el que permite la detección de errores en el

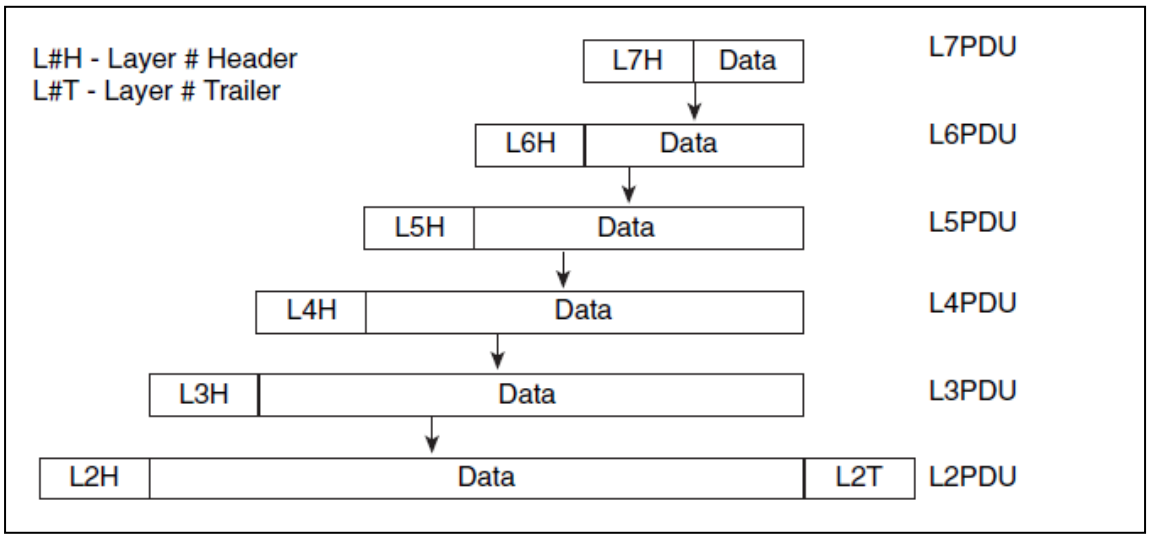
envío de la información. Hay que hacer la aclaración que FCS solo detecta errores pero no los corrige.

La capa física contiene los protocolos que definen el medio por dónde se transmitirá la información, las características materiales, las características funcionales de la interfaz y manejar las señales eléctricas del medio de transmisión.

Son varios los beneficios que presenta un modelo con varias capas, ya que este rompe un sistema complejo con varios protocolos y funciones, y los agrupa en capas o niveles permitiendo de esta manera un mejor manejo de la información así como de su transmisión. Facilita el empleo de hardware y software. La detección y corrección de fallas se hace más simple utilizando la segmentación y agrupación de protocolos.

Algo que no se puede dejar a un lado es la terminología empleada por OSI para cada una de las encapsulaciones como resultado de cada capa. Para esto, OSI define el protocolo de unidad de datos (PDU por sus siglas en inglés). Un PDU es un encapsulado que incluye los encabezados, datos y colas resultado de una capa dada. Por ejemplo, al paquete IP se le denomina PDU de capa tres o como normalmente lo se llama un L3PDU.

Figura 3. **Encapsulación y protocolos de unidad de datos en OSI**



Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p.37.

1.2. Fundamentos de LAN

Se le denomina LAN a una red de área local (Local Area Network) donde se encuentran conectados varios dispositivos terminales que se necesita se comuniquen entre sí. A lo largo de la historia han existido varios tipos de LAN: Token Ring, FDDI, ATM y Ethernet. Al final el gran ganador fue Ethernet por lo que hoy en día cuando se menciona LAN no cabe duda que se está hablando de Ethernet.

Ethernet es una familia de estándares que, en conjunto, definen los medios físicos y enlaces de datos de las redes actuales. Los distintos estándares varían básicamente en función ancho de banda soportado. Actualmente se habla de anchos de nada de 10, 100, 1 000, 10 000 mega bytes por segundo. Otro factor que diferencia un estándar de otro es el medio o canal de comunicación empleado y las distancias que dichos canales soportan. Entre

estos se puede mencionar cables UTP (en sus distintas categorías) y la fibra óptica (con sus distintos modos de operación). En lo que respecta a la capa de enlace de datos, la IEEE separa esta capa en dos subcapas: la 802,3 media access control (MAC) subcapa y la 802,2 Logical Link Control (LLC) subcapa.

Tabla I**.** **Tipos de Ethernet más comunes**

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Copper, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Fiber, 550 m (SX) 5 km (LX)
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	100 m

Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p.36.

Para la construcción de una LAN Ethernet se debe contar con los siguientes elementos: computadoras o dispositivos terminales que tengan una tarjeta de red como interfaz ethernet (NIC), un Switch Ethernet y cables UTP para la conexión entre dispositivos y el Switch.

Figura 4. **Encabezados LAN**

Preamble 7	SFD 1	Destination 6	Source 6	Length/ Type 2	Data and Pad 46 – 1500	FCS 4

Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p. 66.

En la figura 4 se muestra una trama Ethernet, la cual está compuesta de varios campos. Cada campo se explica en la tabla II.

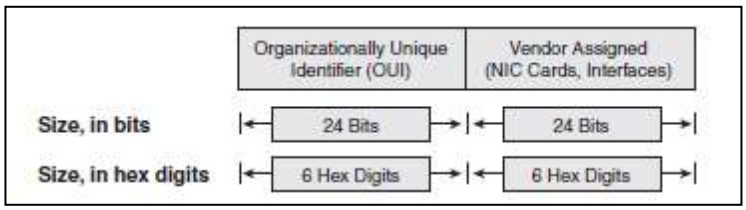
Tabla II. **Campos del encabezado LAN**

Field	Field Length in Bytes	Description
Preamble	7	Synchronization
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC field
Destination MAC address	6	Identifies the intended recipient of this frame
Source MAC address	6	Identifies the sender of this frame
Length	2	Defines the length of the data field of the frame (either length or type is present, but not both)
Type	2	Defines the type of protocol listed inside the frame (either length or type is present, but not both)
Field	**Field Length in Bytes**	**Description**
Data and Pad*	46–1500	Holds data from a higher layer, typically an L3 PDU (generic), and often an IP packet
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine if the frame experienced transmission errors

Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p. 46.

Dados estos campos, vale la pena detenerse un momento en los campos de MAC origen y MAC destino. Cada tarjeta de red posee una dirección MAC que es única e irrepetible.

Figura 5. **Encabezados LAN**



Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p. 64.

En la figura 5 se muestra cómo está formada la dirección MAC. Los primeros 24 bits son un identificador único que es asignado por la IEEE. Los 24 bits restantes son asignados por el fabricador de tarjetas de red.

1.3. Fundamentos de WAN

Se le denomina WAN a una red de área amplia (Wide Area Network) a redes que se extienden sobre un área geográfica extensa. Normalmente este tipo de redes son punto a punto o punto multipunto. A diferencia de las redes LAN, la velocidad a la que circulan los datos por las redes WAN suele ser menor, esto debido a que normalmente una empresa que necesita interconectar dos redes LAN entre si difícilmente tendrá permisos para realizar un cableado por una zona pública o crear en radio enlace para los mismos fines.

Por lo contrario, lo que las empresas optan es por contratar un enlace dedicado por medio de una empresa de telecomunicaciones que ya tiene toda la infraestructura y equipo necesario para realizar estos enlaces. Obviamente la empresa de telecomunicaciones le brinda el mismo servicio a muchas otras empresas más, por lo que los recursos se deben ir compartiendo y se vuelve

muy costoso poder tener un ancho de banda grande o similar al que se puede alcanzar en una LAN.

Cuándo se habla de WAN, normalmente se piensa en un enrutador (*router*), el cuál es el encargado de enrutar la información de un lado a otro atravesando la red de la empresa que brinda el servicio. Normalmente para estos enlaces dedicados se hablaba de redes conmutadas por circuito, y las velocidades a las que se podía optar, ver tabla III:

Tabla III. **Campos del encabezado LAN**

Name(s) of Line	Bit Rate
DS0	64 kbps
DS1 (T1)	1.544 Mbps (24 DS0s, plus 8 kbps overhead)
DS3 (T3)	44.736 Mbps (28 DS1s, plus management overhead)
E1	2.048 Mbps (32 DS0s)
E3	34.064 Mbps (16 E1s, plus management overhead)
J1 (Y1)	2.048 Mbps (32 DS0s; Japanese standard)

Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p. 83.

Dos protocolos son normalmente empleados en redes WAN, punto a punto (PPP) o control de enlace de datos de alto nivel (HDLC).

En la figura 6 se observa que HDLC al igual que Ethernet es capaz de detectar errores por medio del campo FCS.

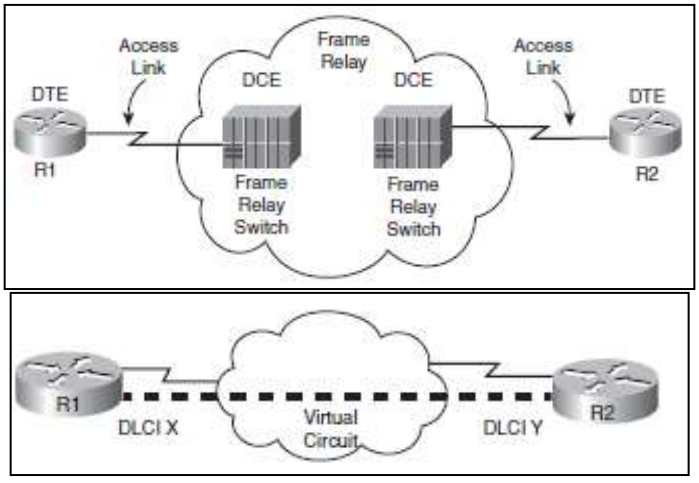
Tabla IV. **Encabezados WAN**

Preamble 7	SFD 1	Destination 6	Source 6	Length/ Type 2	Data and Pad 46 – 1500	FCS 4

Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p. 84.

Por otro lado, se tiene la tecnología Frame Relay, por medio de la cual se tiene una red conmutada por paquetes. Esto se logra creando circuitos virtuales, los cuales establecen una red virtual independiente para los clientes, en la que los clientes de una empresa dada pueden verse entre sí desde varios sitios, mas no se percatan de la presencia de otras redes virtuales montadas sobre la misma red de conmutación brindada por la empresa de telecomunicaciones. Esto brinda una escalabilidad mucho mayor a las redes, ya que por un solo enlace físico se pueden manejar varios circuitos virtuales, lo cual simplifica notablemente la implementación de este tipo de redes.

Figura 6**.** **Topología física/lógica Frame Relay**

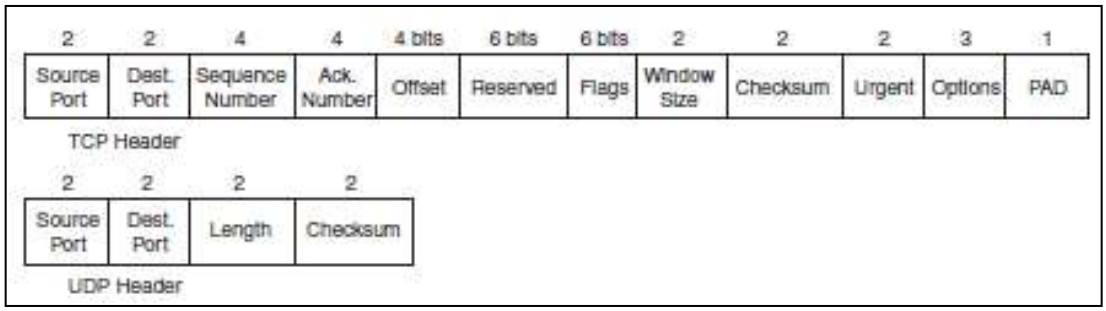


Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p. 88.

1.4. Fundamentos de transporte, aplicación y seguridad sobre TCP/IP

En la capa de transporte se utilizan únicamente dos protocolos, por un lado se tiene TCP que es un protocolo orientado a conexión y UDP que no es un protocolo orientado a conexión.

Figura 7**.** **Encabezado TCP y UDP**

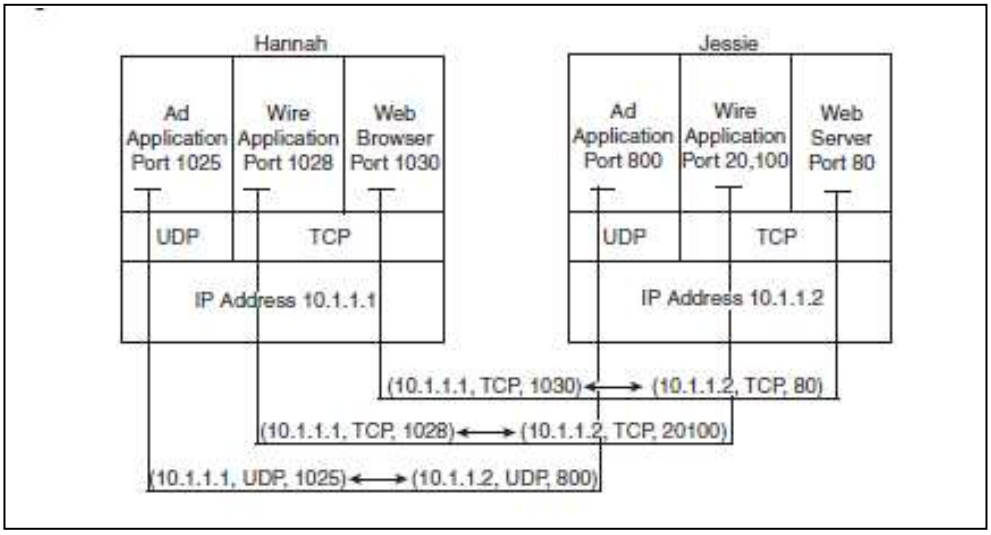


Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p. 522.

Se detalla el encabezado TCP y UDP. Se puede ver a simple vista que el encabezado UDP es mucho más ligero que el protocolo TCP, debido a esto, el tiempo que lleva procesar un encabezado UDP es mucho menor al tiempo que lleva procesar un encabezado TCP. Los campos comunes entre los encabezados TCP y UDP son tres: puerto origen, puerto destino y *checksum*.

Los puertos son utilizados para multiplexzar información enviada por un dispositivo, a manera que cada aplicación que se está ejecutando en el dispositivo etiquetará cada segmento con un puerto origen distinto, esto a manera que cuando el segmento venga de regreso al dispositivo, el dispositivo sea capaz de reconocer que dicha información pertenece a una aplicación en específico. En la figura 9 se puede apreciar bien la función de los puertos:

Figura 8. **Funcionamiento puertos TCP y UDP**



Fuente: ODOM, Wendell. *CCENT/CCNA ICND1.* p 138.

A continuación se muestra la tabla V con puertos que los dispositivos utilizan:

Tabla V. **Listado de puertos comunes TCP y UDP**

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH

Continuación de la tabla V.

Port Number	Protocol	Application
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384–32,767	UDP	RTP-based Voice (VoIP) and Video

Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p. 140.

TCP, a diferencia de UDP, posee la capacidad de detectar errores y de presentarse el caso, pedir una retransmisión para la corrección del mismo. Una de las aplicaciones que utilizan UDP es voz sobre IP, ya que para este tipo de tráfico, no se desea tener muchos tiempos de retraso originados por la red de transporte por lo que UDP es el protocolo de trasporte adecuado para este tiempo de tráfico. DNS y video *streaming* son otro tipo de aplicaciones que hacen uso del protocolo UDP.

El objetivo de implementar una red no es para otra cosa que permitir y brindar la conectividad necesaria para que aplicaciones puedan intercambiar información entre sí. Cada aplicación se puede analizar en términos de sus parámetros de calidad y servicios, los cuáles deben ser reconocidos y aplicados dentro de la red que le brinda el transporte para que todo funcione bien.

Los parámetros básicos son:

- Ancho de banda: cantidad de información que se transmite en un canal de comunicación dado.

- Retraso o latencia: suma de los retrasos que toma la información en llegar de su fuente a su destino.

- El jitter: variación de retrasos que le lleva a un paquete en llegar de una fuente a un destino dado.

- Pérdida de paquetes: término empleado normalmente protocolos no orientados a conexión. Es por eso que todas las aplicaciones en tiempo real están basadas en el protocolo UDP. Este tipo de protocolos no reenvían paquetes perdidos.

Tabla VI. **Características de diferentes tipos de tráfico**

Type of Application	Bandwidth	Delay	Jitter	Loss
VoIP	Low	Low	Low	Low
Two-way video over IP (such as videoconferencing)	Medium/high	Low	Low	Low
One-way video over IP (such as security cameras)	Medium	Medium	Medium	Low
Interactive mission-critical data (such as web-based payroll)	Medium	Medium	High	High

Continuación de la tabla VI.

Type of Application	Bandwidth	Delay	Jitter	Loss
Interactive business data (such as online chat with a coworker)	Low/medium	Medium	High	High
File transfer (such as backing up disk drives)	High	High	High	High
Nonbusiness (such as checking the latest sports scores)	Medium	High	High	High

Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p 149.

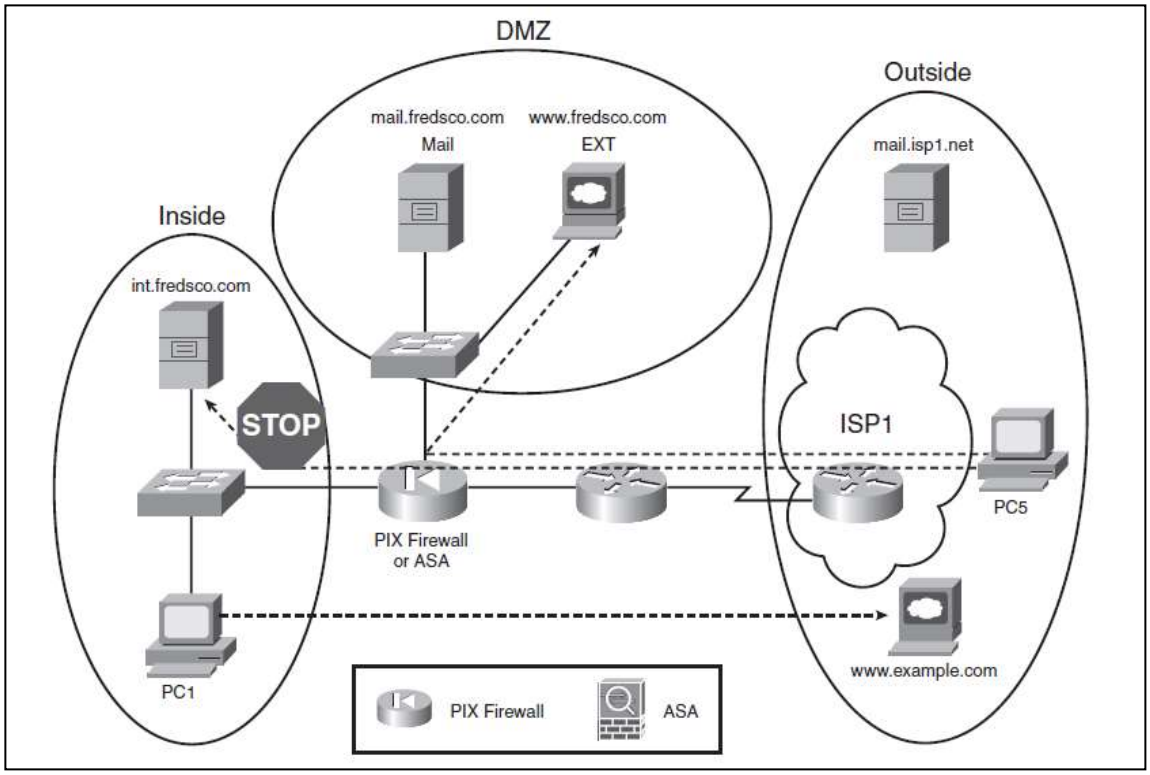
Cuando se busca migrar todas las aplicaciones a un mundo IP, la seguridad de en la red se torna vital. Históricamente han existido personas que buscan atacar redes por el simple hecho de demostrar que son capaces de ingresar a redes que llaman seguras.

El problema actual radica en que ya no se necesita de algún grado académico o experiencia, hoy en día existen programas gratuitos que cualquier persona sin tener un alto grado de conocimiento en el área puede descargar y descubrir cómo se usa para poder hacer algún tipo de daño a una red. Este tipo de circunstancias vuelven de internet un entorno altamente inseguro, por lo que es obligación tanto de las empresas como se los proveedores de servicio de brindar, en lo que a ellos confiere, una red segura.

El equipo históricamente que se ha utilizado para poder brindar seguridad a las empresas es un Firewall, el cual hace una división entre una zona inside donde residen todos los equipos donde se tienen aplicadas políticas de alta seguridad, para alguien que intente ingresar a dichos equipos desde afuera de la red, una zona outside que es típicamente internet y una zona desmilitarizada

(DMZ) donde se ubican los equipos a los que normalmente se desea se tenga acceso desde afuera de la red.

Figura 9. **Arquitectura de seguridad**



Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p 139.

Se estima que el 68 por ciento de los ataques a la red de una empresa son internos, ya sea por algún empleado disgustado, una computadora móvil que traiga algún tipo de virus de afuera y en el caso de las empresas que cuentan con redes inalámbricas, como estas muchas veces son detectadas desde afuera del edificio, cualquier persona en las afueras podría conectarse y entrar desde allí a la red de la empresa.

Los ataques de red se clasifican por sus efectos, en: reconocimiento, acceso y denegación de servicios. Los ataques de reconocimiento y acceso son muy comunes en temas de espionaje y aplicaciones financieras. La denegación de servicios busca el bloqueo de servicios a usuarios así como la destrucción parcial y total de información que reside en granjas de servidores.

2. PROTOCOLO IP EN REDES DE DATOS

El protocolo IP es un protocolo no orientado a conexión que se utiliza para la comunicación de equipos terminales a través de una red de paquetes conmutados no fiable de mejor entrega posible sin garantías, de esta manera el protocolo IP provee un servicio de datagramas no fiable, haciendo lo mejor posible pero garantizando poco.

2.1. Fundamentos protocolo IP

La información a transmitir es dividida en paquetes de un determinado tamaño (MTU) y estos paquetes (datagramas) son enviados por caminos distintos, dependiendo de cómo estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen direcciones origen y destino de los equipos terminales que se desean comunicar (direcciones IP), direcciones que son utilizadas por los enrutadores para decidir el tramo de red por el que se reenviarán los paquetes.

El protocolo IP no garantiza nada sobre la recepción de un paquete, por lo que existe la posibilidad de que un paquete llegue dañado, llegue duplicado o simplemente no llegue a su destino. Si se necesita fiabilidad, esta es proporcionada por los protocolos de la capa de transporte, como TCP.

2.2. IPv4

El protocolo IP en su versión 4 es el protocolo que se utiliza actualmente en la mayoría de redes. Este protocolo, aunque en su versión cuatro, es la primera versión en ser implementada a gran escala. Este protocolo está definido en el RFC 791.

IPv4 utiliza direcciones de 32 bits, limitando las direcciones a 2^32 = 4 294 297 296 direcciones únicas muchas de las cuales están dedicadas a redes locales (LAN).

2.2.1. Cabecera IPv4

Si bien las direcciones IPv4 son de 32 bits, el encabezado IPv4 ocupa 20 bytes (160 bits). El significado de cada uno de los campos que componen el encabezado es como sigue:

- Versión, aquí se especifica la versión del protocolo IP. La mayoría de redes actuales utilizan la versión 4.

- IP Header Length (IHL), indica la longitud total del encabezado IP incluyendo opciones de campo adicionales.

- Differentiated Services (DS) Field, es utilizado para el marcaje de paquetes a nivel IP con el objetivo de poder aplicar diferentes políticas de calidad de servicio a paquetes provenientes de una misma fuente pero asociados a flujos de tráfico distintos.

- *Packet length,* indica la longitud completa del paquete IP.

- *Identification,* es utilizado cuando existe un proceso de fragmentación del paquete IP, todos los paquetes IP pertenecientes al mismo paquete original contienen el mismo número de identificación.

- *Flags*, emplea 3 bits que se usan durante un proceso de fragmentación.

- *Fragment offset,* es empleado en el proceso de reagrupación de un paquete previamente fragmentado.

- Time To Live (TTL), es utilizado para prevención de loops de capa 3 entre enrutadores.

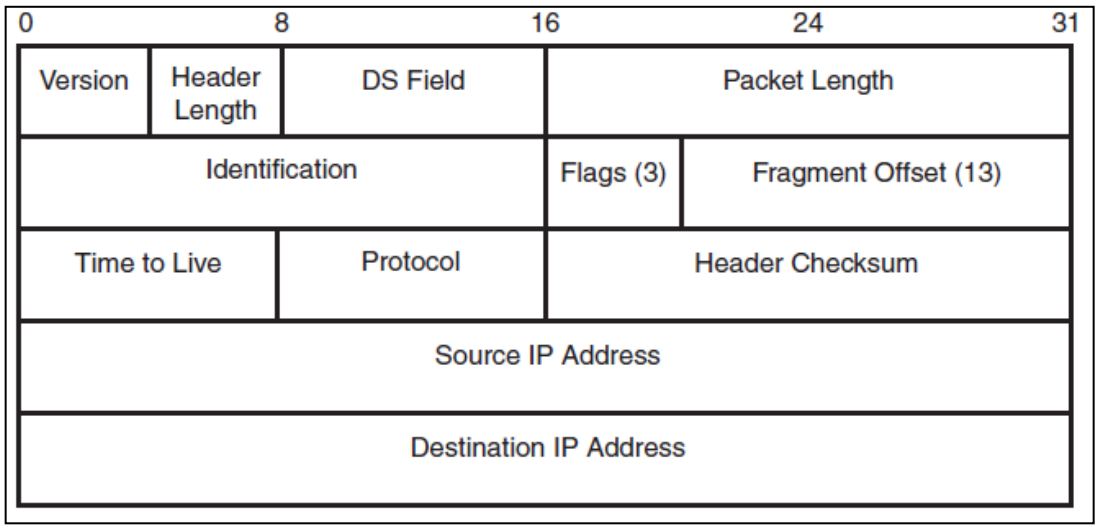
- *Protocol,* identifica el protocolo empleado en el siguiente encabezado dentro de la data del paquete IP. Es muy común encontrar aquí indicadores de que el siguiente protocolo sea TCP o UDP.

- *Header Checksum,* contiene un valor FCS con el propósito de poder determinar si ha ocurrido algún error en cualquiera de los bits del encabezado IP.

- *Source IP address*, contiene la dirección origen IPv4 de 32 bits.

- *Destination IP address,* contiene la dirección destino IPv4 de 32 bits.

Figura 10. **Cabecera paquete IPv4**



Fuente: ODOM, Wendell. CCENT/CCNA ICND1. p. 102.

2.2.2. Direccionamiento IPv4

Las direcciones IPv4 tienen una longitud de 32 bits que a su vez está dividida en 4 octetos, cada uno separado por un punto.

Para cada octeto se utiliza notación decimal, por lo que cada octeto puede variar desde 0 a 255. 72.34.25.21 es un ejemplo de dirección IPv4, la misma dirección en binario sería 01001000.00100010.00011001.00010101

Cada interfaz de red utiliza una dirección IP que en principio, debería de ser única. Dado si una computadora contiene dos tarjetas de red, tendrá dos direcciones IP distintas. En un enrutador, por ejemplo, cada interfaz tiene una dirección IP distinta.

Una dirección IP se separa en dos partes: una parte representa la red y la otra parte representa el *host*. Con base en esto hay tres tipos de direcciones: clase A, clase B y clase C.

La clase A utiliza solo el primer octeto para identificar la red y tres octetos para *host.* De esta cuenta se tienen 16 777 214 direcciones IP por red y 127 redes clase A.

La clase B utiliza dos octetos para identificar la red y dos octetos para *host*. De esta cuenta se tienen 65 534 *host* por red y 16 384 redes clase B.

Por último se tiene la clase C, la cual utiliza 3 octetos para red y un octeto para *host.* De esta cuenta se tienen 254 *host* por red y hasta 2 097 152 de redes clase C.

Adicional a las tres clases ya definidas, se tienen dos clases más: D y E. La clase D es usada para multicast y la E está reservada para usos experimentales.

Cada segmento de red cuenta con una dirección de red y una dirección *broadcast*. Estas dos direcciones no son utilizables y no pueden ser asignadas a equipos terminales o *host*.

Una parte muy importante de la dirección IP es la máscara, ya que es esta la encargada de indicar, de una dirección IP, cuantos bits corresponden a la red y cuántos al *host*. La clase A utiliza una máscara 255.0.0.0, la clase B utiliza una máscara 255.255.0.0 y la clase C una máscara 255.255.255.0.

El enrutador realiza una operación de AND entre la dirección IP y la máscara para determinar cuál es la red donde se encuentra un host.

2.3. IPv6

El protocolo IP en su versión 6 fue desarrollado por la IETF para tratar con la ya anticipada extinción de direcciones IPv4. Este protocolo está definido en el RFC 2460.

A diferencia de IPv4, IPv6 cuenta con 2^128 direcciones de red, lo cual es un número elevadísimo de direcciones IP.

2.3.1. ¿Por qué IPv6?

Si bien se pensó en un inicio que el dimensionamiento de direcciones IPv4 era el adecuado, hoy en día se ve la necesidad de ampliar el rango de direcciones IP. Incluso durante un tiempo se pensó que mediante la optimización del uso de las direcciones IPv4, la implementación de NAT y la recuperación de direcciones no utilizadas se podía resolver la demanda de direcciones IP sin la necesidad de adoptar una nueva versión del protocolo.

Sin embargo, con forme ha pasado el tiempo, esta idea se ha ido desvaneciendo, y la necesidad de una nueva versión del protocolo se ha vuelto un tema más que una opción, una necesidad para resolver la demanda de direcciones IP.

Otro aspecto muy importante por el cual la implementación de NAT no es una solución adecuada en muchos escenarios es que se dificulta el despliegue

de aplicaciones y servicios extremo a extremo, haciendo más costoso y complejo el desarrollo de este tipo de servicios y aplicaciones.

2.3.2. Cabecera IPv6

Un paquete IPv6 se conforma por dos partes: la cabecera y la carga útil.

Dentro de la cabecera se encuentra una parte fija y otra parte que es opcional y se puede utilizar para varias opciones llamada cabecera de extensiones.

La parte fija de la cabecera está conformada por 40 bytes (320 bits) y contiene los siguientes campos:

Figura 11. **Cabecera paquete IPv6**

<table>
<tr><th rowspan="2">Offset del Octeto</th><th colspan="2">0</th><th colspan="2">1</th><th colspan="2">2</th><th colspan="2">3</th></tr>
<tr><th>Bit Offset</th><th>0 1 2 3 4 5 6 7</th><th>8 9 10 11 12 13 14 15</th><th>16 17 18 19 20 21 22 23</th><th>24 25 26 27 28 29 30 31</th></tr>
<tr><td>0</td><td>0</td><td>Versión</td><td colspan="2">Clase de Tráfico</td><td colspan="3">Etiqueta de Flujo</td></tr>
<tr><td>4</td><td>32</td><td colspan="3">Longitud del campo de datos</td><td>Cabecera Siguiente</td><td>Límite de Saltos</td></tr>
<tr><td>8</td><td>64</td><td colspan="5" rowspan="4">Dirección de Origen</td></tr>
<tr><td>C</td><td>96</td></tr>
<tr><td>10</td><td>128</td></tr>
<tr><td>14</td><td>160</td></tr>
<tr><td>18</td><td>192</td><td colspan="5" rowspan="4">Dirección de Destino</td></tr>
<tr><td>1C</td><td>224</td></tr>
<tr><td>20</td><td>256</td></tr>
<tr><td>24</td><td>288</td></tr>
</table>

Fuente: elaboración propia.

El significado de cada uno de los campos que componen el encabezado es como sigue:

- Versión, campo de 4 bits es donde se indica la versión del protocolo IP que se está empleando. En el caso de IPv4 es el número 4 (0100) y en el caso de IPv6 es el número 6 (0110).

- Clase de tráfico, campo de 8 bits, puede adquirir varios valores de manera que sea posible la separación de tráficos de una misma fuente con el objetivo de poder brindar diferentes servicios de entrega para cada uno de los tráficos, algo que comúnmente se le lleva calidad de servicio diferenciado.

- Etiqueta de flujo, campo de 20 bits le permite a los enrutadores tener la capacidad de poder etiquetar los distintos tipos de flujos de tráfico. Permitiendo asociar cada paquete IPv6 a un único tipo de tráfico y poder garantizar una misma política de calidad de servicio desde el origen hasta el destino. Esta etiqueta permite llevar un control de cada flujo de tráfico, muy similar a lo que hace el protocolo de reserva de recursos (RSVP, por sus siglas en inglés).

- Longitud de campo, campo de 16 bits, contiene la longitud de la data dentro del paquete luego del encabezado. El límite es de 64 kilobytes. En caso de que se requiera un campo con una mayor longitud se requiere de un encabezado de extensión empleado para jumbogramas. Esto se indica con un valor de cero en el campo longitud de campo de datos.

- Cabecera siguiente, campo de 8 bits, es empleado para indicar el tipo de encabezado que le sigue al encabezado IPv6. Los más comunes son TCP (6) y UDP (17).

- Límite de saltos, campo de 8 bits, es un valor que va en decremento en cada salto que el paquete da por un enrutador. Es un mecanismo de prevención de *loops* en capa 3 entre enrutadores.

- Dirección de origen, contiene la dirección origen IPv6 de 128 bits.

- Dirección de destino, contiene la dirección destino IPv6 de 128 bits.

2.3.2.1. Cabeceras de extensiones

La cabecera de extensiones es una idea innovadora que permite ir añadiendo funcionalidades de una manera paulatina lo cual brinda una gran eficacia y flexibilidad y se ubica entre la cabecera fija y la carga útil.

Hasta el día de hoy, se encuentran 8 tipos de cabeceras de extensión:

Tabla VII. **Cabeceras de extensión**

Name(s) of Line	Bit Rate
DSO	64 kbps
DSl (Tl)	1,544 mbps (24 DSOs, plus 8 kbps overhedad
DS3(T1)	44,736 Mbps (28 DS1s, plus management overhead)
El	2,048 Mbps (32 DSOs)
E3	34,064 Mbps (16 Els, plus management overhead)
Jl(Yl)	2,048 Mbps (32 DSOs; Japanese standard)

Fuente: www.ipv6.com/articles.com. Consulta: 12 de enero de 2014.

2.3.3. Direccionamiento IPv6

El hecho que las direcciones pasen de los 32 bits a los 128 bits, hace que desaparezcan los problemas de direccionamiento IPv4 actual y consecuentemente que no sean necesarias técnicas de NAT IPv4 para proporcionar conectividad a todos los ordenadores/dispositivos de la red.

En IPv6 se tienen tres tipos direcciones: Unicast, Anycast y Multicast.

Las direcciones Unicast se emplean como identificador para una única interfaz. Un paquete enviado a una dirección Unicast es entregado solo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

Las direcciones Anycast se emplean como identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección Anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Permite crear, por ejemplo, ámbitos de

redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el protocolo de ruteo), si la primera cae.

Las direcciones Multicast se emplean como identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección Multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (*broadcast*).

2.3.3.1. Representación de direcciones IPv6

La representación de las direcciones IPv6 es el sucesor del primer protocolo de direccionamiento de internet, internet Protocol versión 4 se hace bajo el siguiente esquema:

x:x:x:x:x:x:x

Donde x es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A

Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits cero, se permite la escritura de su abreviación, mediante el uso

de ::, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPv6.

Ejemplos:

Las direcciones:

1080:0:0:0:8:800:200C:417A (una dirección unicast)
FF01:0:0:0:0:0:0:101 (una dirección multicast)
0:0:0:0:0:0:0:1 (la dirección *loopback*)
0:0:0:0:0:0:0:0 (una dirección no especificada)
Pueden representarse como:

1080::8:800:200C:417A (una dirección unicast)
FF01::101 (una dirección multicast)
::1 (la dirección *loopback*)
:: (una dirección no especificada)

Una forma alternativa y muy conveniente, cuando se halle en un entorno mixto IPv4 e IPv6, es

x:x:x:x:x:x:d:d:d:d

Donde x representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y d representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4).

Ejemplos:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

Pueden representarse como:

::13.1.68.3
::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo: dirección-IPv6/longitud del prefijo, donde la dirección-IPv6 es una dirección IPv6 en cualquiera de las notaciones válidas y la longitud del prefijo es un valor decimal, indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo.

2.3.3.2. Criterios de asignación de direccionamiento IPv6

A los ISP que tengan previsto conectar a más de 200 redes finales (sitios finales) en 2 años se les asigna un bloque /32 de direcciones IPv6.

Para la asignación a redes finales (sitios finales) en general se asigna un bloque /48 para grandes y medianas empresas así como para redes domésticas. En el caso que exista solo una subred, como por ejemplo redes móviles, un bloque /64 es lo que se le asigna normalmente.

2.4. Enrutamiento IPv6

El enrutamiento es el proceso de reenviar paquetes entre segmentos de red conectados. En las redes basadas en IPv6, el enrutamiento es la parte de IPv6 que proporciona capacidades de reenvío entre *hosts* que se encuentran en segmentos independientes que pertenecen a una red mayor basada en IPv6.

IPv6 es la oficina de correos donde se ordenan y entregan los datos de IPv6. Cada paquete entrante o saliente se denomina paquete IPv6. Un paquete IPv6 contiene la dirección de origen del *host* que realiza el envío y la dirección de destino del *host* receptor. A diferencia de las direcciones de nivel de vínculo, las direcciones IPv6 del encabezado IPv6 no suelen cambiar cuando el paquete se transmite por una red IPv6.

El enrutamiento es la función principal de IPv6. Los paquetes IPv6 se intercambian y procesan en cada *host* mediante IPv6 en el nivel de internet.

Por encima del nivel IPv6, los servicios de transporte del *host* de origen pasan los datos en forma de segmentos TCP o mensajes UDP al nivel IPv6. El nivel IPv6 crea los paquetes IPv6 con la información de las direcciones de origen y destino, que se utiliza para enrutar los datos a través de la red. Después, el nivel IPv6 pasa los paquetes al nivel inferior del vínculo, donde los paquetes IPv6 se convierten en tramas para su transmisión a través de los medios específicos de una red física. Este proceso se produce en el orden inverso en el *host* de destino.

En cada *host* remitente, los servicios del nivel IPv6 examinan la dirección de destino de cada paquete, comparan esta dirección con una tabla de enrutamiento mantenida localmente y, después, determinan qué acción de

reenvío adicional es necesaria. Los enrutadores IPv6 están conectados a dos o más segmentos de red IPv6 habilitados para reenviar paquetes entre ellos.

2.4.1. ICMP y los mensajes de error

El objetivo del Internet Control Messagem Protocol es el de enviar mensajes entre equipos, este protocolo se utilizada en la versión 4 de IP, pero para versión ha sufrido un poco de cambios, se puso un formato fijo que es más fácil de manejar por los enrutadores, se le aumentó la capacidad en las direcciones a 128 bits y se quitaron mensajes redundantes o que no se utilizaban.

Tabla VIII. **Códigos más relevantes del ICMPv2**

Codigo	Significado
1	Destino inalcanzable (Destination Unrechable).
2	Paquete demasiado grande (Packet too big).
3	Tiempo de respuesta agotado (Time Exceded).
4	Parámetros incorrectos (Parameter Problem).
128	Solicitud de ECHO (ECHO Request).
129	Respuesta a ECHO (ECHO reply).
133	Solicitud de ruteador (Ruteador Solicitation).
135	Solicitud de vecino (Neighbor Solicitation).

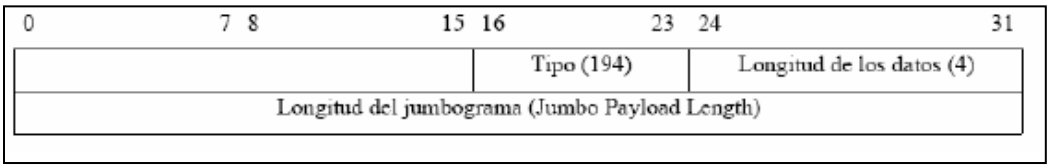
Fuente: AHUATZIN SÁNCHEZ, Gerardo L. *Desarrollo de un esquema de traducción de direcciones* IPv6-IPv4-IPv6. p. 20.

2.4.2. Los jumbogramas

Una mejora interesante y con visión a futuro de IPv6 es la capacidad de manejar cantidades de datos superiores a los 64 kilobytes, en estos momentos no se utiliza porque las redes actuales no pueden manejar más de 64 kilobytes.

El encabezado es como se muestra en la figura 12:

Figura 12. **Encabezado de un jumbograma**



Fuente: AHUATZIN SÁNCHEZ, Gerardo L. *Desarrollo de un esquema de traducción de direcciones* IPv6-IPv4-IPv6. p. 23.

En los foros de Internet y en la IETF, el uso de los jumbogramas ha sido ampliamente discutido y finalmente aceptado por su poca probabilidad de uso a corto plazo.

La discusión es por el principio de transmisión de datos cortos, ya que si se envían N bytes de información y solo un bit se pierde en el camino, se tiene que reenviar todo el paquete; si se tienen paquetes grandes, se reenviarán paquetes grandes y si se tienen paquetes se reenviarán paquetes cortos sin causar tanto tráfico en la red.

3. TÉCNICAS DE TRANSICIÓN IPV4 A IPV6

IPv6 es una nueva versión del protocolo de internet diseñada para suceder a la actual IPv4 y dicha transición entre ambas será un largo proceso durante el que se ha de garantizar la coexistencia.

La migración a la nueva versión del protocolo de internet en tan corto período de tiempo requeriría la redefinición de un plan de direccionamiento IPv6 mundial, la instalación del protocolo en cada enrutador y *host,* y la modificación de las aplicaciones actuales para que puedan soportarlo. Un proceso caro, sin duda, y que podría causar interrupciones del servicio inaceptables. Sencillamente, tal enfoque no tendría sentido, ya que muchas de las aplicaciones operativas actuales no han sido diseñadas para aprovechar las nuevas características de IPv6; ni siquiera las necesitan.

No hay una regla universal que pueda ser aplicada al proceso de transición de IPv4 a IPv6. En algunos casos, adoptar directamente, sin pasos previos, el nuevo IP será la única solución. En Asia, por ejemplo, las autoridades políticas están impulsando fuertemente IPv6 a fin de sostener el crecimiento económico de la zona, garantizando a cada ciudadano un número suficiente de direcciones IP. Asimismo, se ha de desplegar a gran escala una nueva arquitectura IP (como en el *networking* doméstico móvil) para proporcionar aplicaciones peer-to-peer y servicios innovadores.

Pero otros planes de transición habrán de asegurar una interoperatividad gradual entre IPv4 y IPv6 a medida que evoluciona la transición. Es obvio que los ISP y las empresas preferirán preservar las grandes inversiones realizadas

en redes IPv4. Los mecanismos propuestos en este documento permitirán interconectar redes IPv4 e IPv6, así como servidores y clientes basados en ambas versiones.

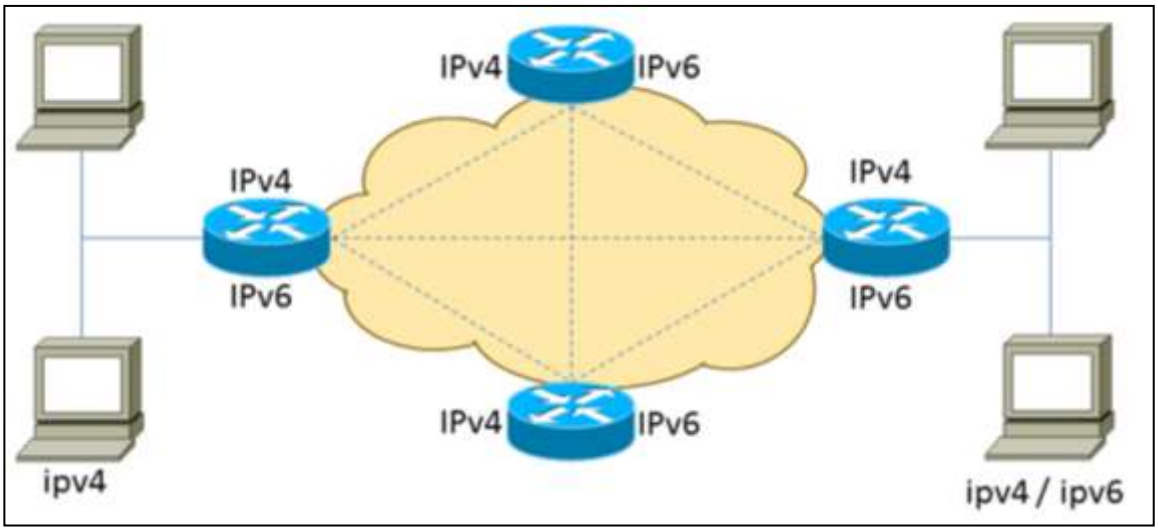
Algunos estudios pronostican que el periodo de transición finalizará entre 2030-2040; en algún momento de esa década, las redes IPv4 deberían haber desaparecido totalmente. Una historia realmente larga comparada con el rápido crecimiento experimentado por internet.

3.1. Técnica de doble pila

Esta técnica da un enfoque muy sencillo de implementar que requiere que los *hosts* y los enrutadores soporten ambas versiones de IP y, por tanto, servicios y aplicaciones tanto IPv4 como IPv6.

En estos momentos, este enfoque de doble pila es un mecanismo fundamental para introducir IPv6 en las arquitecturas IPv4 actuales y se estima que siga siendo muy utilizado durante el próximo futuro. Su punto flaco es que obliga a que cada máquina retenga una dirección IPv4, cada vez más escasas. Así, a medida que se difunde IPv6, la técnica de doble pila tendrá que ser aplicada allí donde específicamente ayuda al proceso de transición, por ejemplo, en enrutadores y servidores. De esta manera se podría pensar en un servidor de doble pila que puede soportar clientes solo IPv4 convencionales, nuevos clientes sólo IPv6, y por supuesto clientes de doble pila.

Figura 13. **Diagrama de red con *Dual Stack***



Fuente: elaboración propia.

Los nodos con ambas pilas de protocolos se denominan nodos IPv6/IPv4. Al utilizar este mecanismo de pilas dobles se tiene una dirección en cada pila. Estas direcciones IPv4 e IPv6 puede que estén relacionadas entre ellas mismas, pero no es un requisito de implementación de este método, por lo que estas direcciones pueden no tener ninguna relación.

Para obtener una dirección IPv6, dichos nodos pueden utilizar los mecanismos de autoconfiguración sin estado o mediante DHCPv6, y para la obtención de su dirección IPv4 pueden utilizar los mecanismos o protocolos estándar como DHCPv4, protocolo de arranque (BOOTP), protocolo de resolución de direcciones inverso (RARP) o la configuración manual en el nodo de la dirección IPv4.

Para que estas direcciones IPv4 e IPv6 estén relacionadas de cierta forma dentro de cada nodo, se puede hacer uso de las direcciones IPv6 compatibles

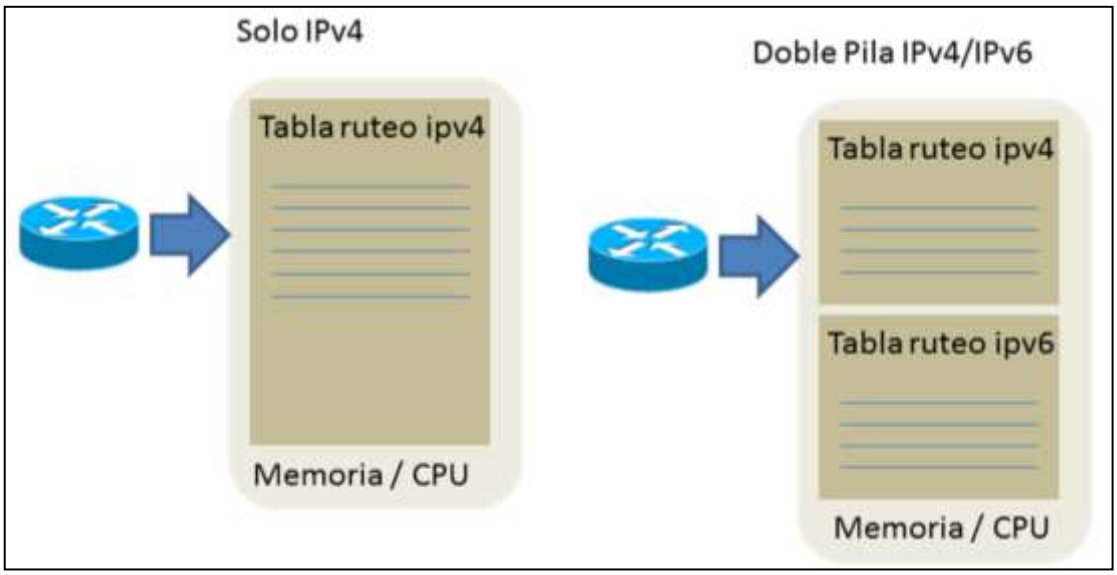
con IPv4. Una dirección de este tipo tiene en sus 96 bits de orden mayor (los de la izquierda) un valor de 0:0:0:0:0:0 y en los 32 bits de menor orden (los de la derecha) una dirección IPv4. Así, al utilizarlas, se podría tener en la pila de IPv6, la dirección que comprende los 96 bits con valor de 0:0:0:0:0:0 más la dirección IPv4, y en la pila de IPv4 la dirección IPv4 que se encuentra en los 32 bits de orden menor de la dirección IPv6.

Figura 14**.** **Mapeo de una dirección IPv4 a IPv6**

Fuente: elaboración propia.

El desafío con *dual stack* es que todos los equipos de la red han de contar la suficiente potencia de proceso y memoria, para gestionar dos pilas IP diferentes. Además, gestionar dos pilas IP supone un doble gasto en gestión y soporte, lo que incrementa los costos de TI.

Figura 15. **Utilización de memoria y CPU con *Dual Stack***



Fuente: elaboración propia.

En resumen, se puede decir que con *Dual stack* se encuentran las siguientes características:

- Todos los equipos P y PE están en la capacidad de soportar tanto direccionaccionamiento IPv4 e IPv6.

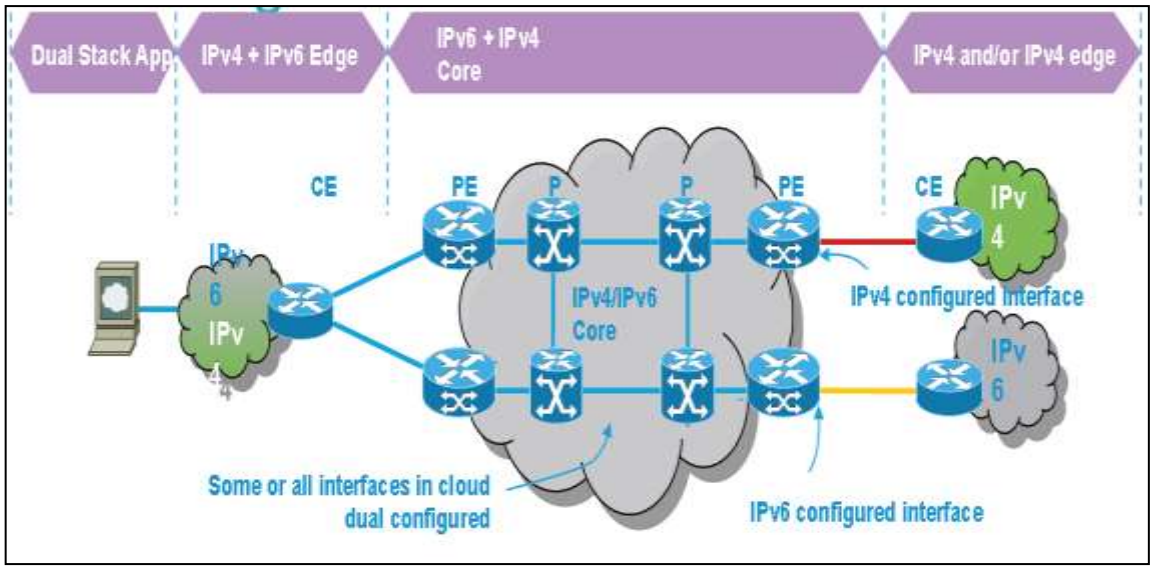
- Se tienen dos procesos de ruteo operando en paralelo para poder manejar prefijos IPv4 e IPv6.

- Una de las consideraciones principales a tomar en cuenta es la utilización de memoria en los equipos debido a las grandes tablas de ruteo que deberán manejar.

- La red es capaz de manejar tráfico nativo multicast IPv6.

- Todo el tráfico IPv6 deberá ser ruteado de manera global dentro de la red.

Figura 16. **Diagrama de red con traductores**



Fuente: elaboración propia.

Los procesos y topologías de ruteo en el Core de una red *Dual Stack* tienen ciertas comparaciones.

Tabla IX. **Protocolos de ruteo en una red *Dual Stack***

IPv4	IPv6	Proceso / Topología
OSPFv2	IS-IS	Separado / Separado
OSPFv2	OSPFv3	Separado / Separado
IS-IS	OSPFv3	Separado / Separado
IS-IS	IS-IS	Común / Común
MT IS-IS	MT IS-IS	Común / Separado

Fuente: elaboración propia.

En los congresos en los que se ha participado relacionados a temas de *Dual Stack,* la tendencia de los proveedores de servicio es a manejar OSPFv2 y OSPFv3 como sus protocolos de ruteo para IPv4 e IPv6 respectivamente. En segundo lugar IS-IS para ambos protocolos y las demás combinaciones por complejidad a nivel de operación no los recomiendan para proveedores de servicio.

Tabla X. **Protocolos recomendados para redes *Dual Stack***

IPv4	IPv6	Proceso / Topología
OSPFv2	IS-IS	Separado / Separado
OSPFv2	OSPFv3	Separado / Separado
IS-IS	OSPFv3	Separado / Separado
IS-IS	IS-IS	Común / Común
MT IS-IS	MT IS-IS	Común / Separado

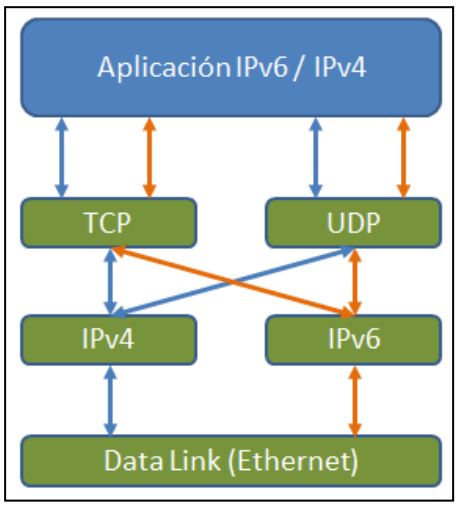
Fuente: elaboración propia.

Cuando se menciona *Dual Stack* en los dispositivos terminales se hace referencia a los siguientes aspectos:

- El dispositivo terminal es capaz de inicar una sesión con IPv4 o IPv6.
- Las aplicaciones que estan instaladas en los dispositivos terminales son capaces de manejar IPv4 o IPv6.
- La decisión de cuando emplear IPv4 o IPv6 es basada en las resoluciones DNS.

Dual Stack en el borde de una red no implica tener *Dual Stack* en el core del mismo.

Figura 17. **Flujo de información con *Dual Stack* en dispositivos terminales**



Fuente: elaboración propia.

3.1.1. Configuración *Dual Stack*

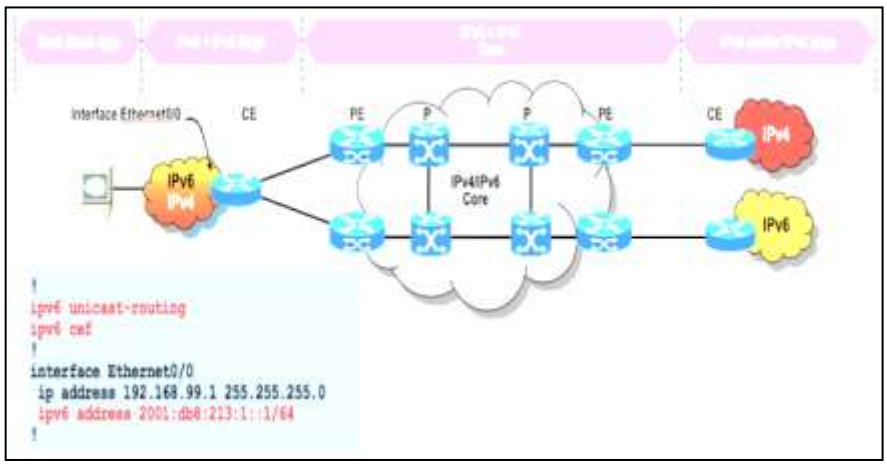
Al momento de configurar equipos de red para que operen en la modalidad Dual Stack, se debe tener en cuenta que en todas las interfaces que interconectan a los equipos entre sí es mandatorio configurar dos direcciones IP, una IPv4 y otra IPv6 todo esto dentro de la misma interfaz física.

- A nivel global en el equipo se debe habilitar el protocol IPv6.

- En caso de que el equipo a configurar sea Cisco, y como una buena práctica, se recomienda habilitar CEF para IPv6, esto de igual manera se hace de manera global.

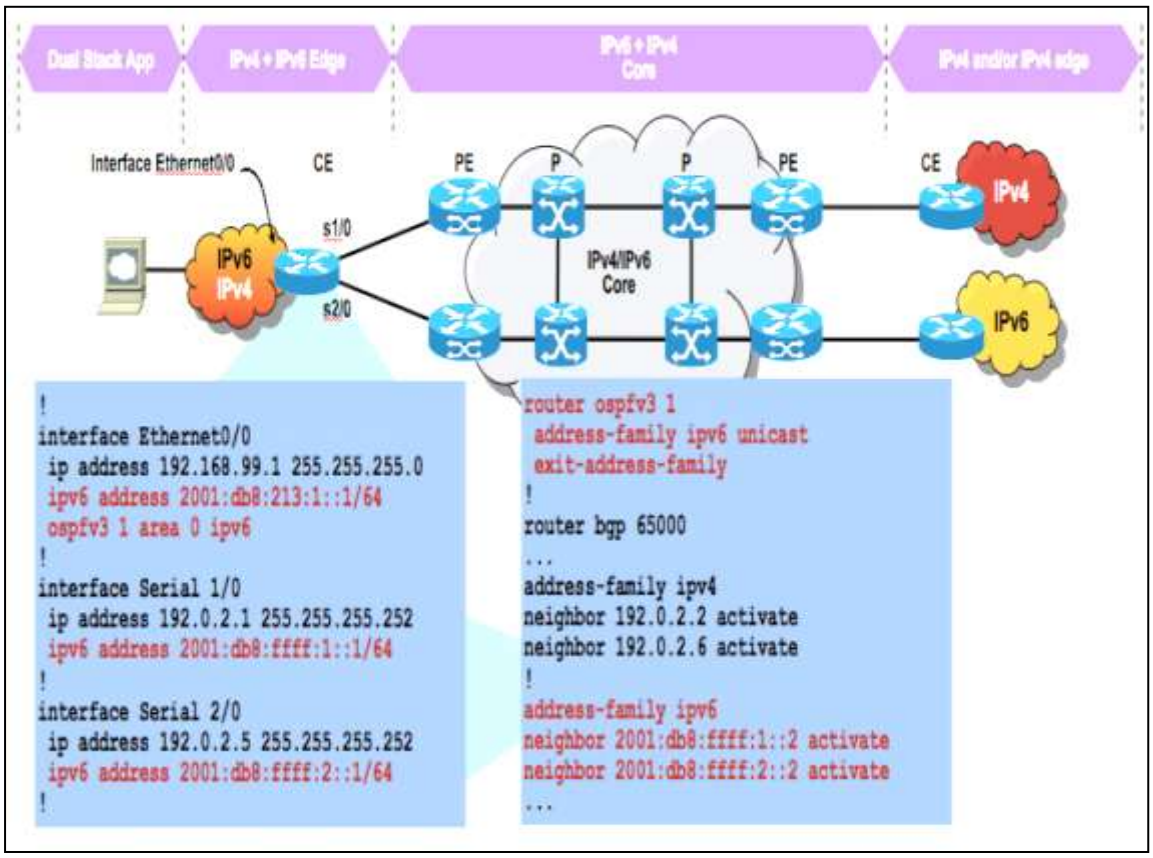
En las figuras 18 y 19 se presenta un ejemplo de cómo es la configuración básica necesaria para implementar *dual stack* en un equipo.

Figura 18. **Configuración de direccionamiento IPv4 – IPv6 Interfaz usuario**



Fuente: elaboración propia.

Figura 19. **Configuración protocolos de ruteo en red ISP**



Fuente: elaboración propia.

En las figuras 20 y 21 se puede observar:

- Las tres interfaces del equipo configurado fueron configuradas con direccionamento IPv4 e IPv6 como era de esperarse.

- En las interfaces seriales que ven a la red del proveedor de servicio, adicional a las dirreciones IPv4 e IPv6 se les ha configurado OSPFv3 lo que indica que para efectos de ruteo a nivel IPv6 se tendrá un IGP dinámico, en este caso OSPF. Luego a nivel global se declara el proceso

OSPF respectivo en dónde se define el *address-family* ipv6 *unicast* el cuál hace referencia a los vecinos con los que se intercambiará tablas de ruteo IPv6.

- A nivel global se ha habilitado ipv6 *unicast-routing,* lo cuál habilita en el equipo todos los comandos y procesos propios de IPv6, para efectos de las figuras serían todos los comandos en color rojo.

- Por ser un equipo Cisco, se habilita CEF para IPv6, esto mejora el rendimiento del equipo a la hora de enrutar paquetes IPv6, sin embargo es una buena práctica más no un comando mandatorio para habilitar IPv6 en el equipo.

- Los prefijos que se han configurado para las direcciones IPv4 son /24 en lo que para IPv6 ha sido /64 como era de esperarse.

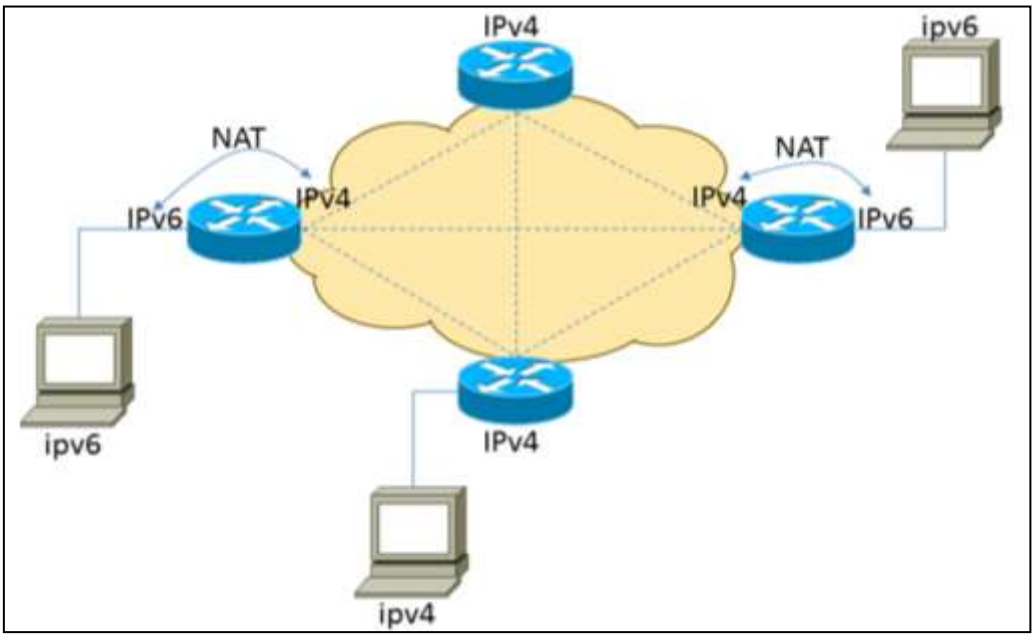
3.2. Técnicas basadas en traductores

Es un desarrollo relativamente reciente, y ya se ha convertido en toda una revolución para la migración de los dispositivos. Una vez que fue considerada la herramienta de último recurso por la IETF (Internet Engineering Task Force), los esquemas de traducción están empezando a ser muy populares a la hora de abordar muchas transiciones. La tecnología de traducción es utilizada cuando un único host IPv6 necesita comunicarse con otro IPv4 o viceversa. Este método de migración es la única de las soluciones en IPv6 que permite eliminar definitivamente el direccionamiento IPv4 de los nodos de red.

Esto ofrece ventajas muy significativas respecto a otras soluciones de migración, como por ejemplo, la posibilidad de integrar sistemas IPv6 nativos en redes que aún mantienen en soporte para dispositivos IPv4 más antiguos. Además, mantiene la seguridad punto a punto de la conexión. Un aspecto crítico de la tecnología de traducción es su enfoque *single-stack*, que reduce al mínimo la cantidad de hardware necesario (que funciona de manera nativa en IPv6 o IPv4), lo que reduce la cantidad de recursos de TI necesarios para mantener la red de datos.

El enfoque *single-stack* ofrece un modo simple y más económico, para manejar redes nativas en IPv6. Tan pronto como las aplicaciones IPv6 aparezcan, los departamentos de TI simplemente tienen que eliminar el viejo hardware IPv4 y reemplazarlo por otro nuevo con protocolo IPv6.

Figura 20. **Diagrama de red con traductores (NAT6to4)**



Fuente: elaboración propia.

3.3. Técnica basada en túneles de IPv4

Los túneles son mecanismos de transición que permiten que los paquetes puedan encapsularse con el objetivo principal de atravesar redes con características diferentes. A nivel macro, los túneles pueden dividirse en dos grandes grupos:

- Túneles configurados (manuales): tal y como su nombre lo indica, se configuran den manera manual tanto en un extremo como el otro del túnel. Esta solución, si bien funciona, impone establecer el túnel de una manera estática con algún dispositivo remoto que pueda proveer conexión hacia redes IPv6. Aunque son sencillos, no brindan alta disponibilidad al momento de una falla en la red, lo cual no solo complica el tema de operación y mantenimiento de la misma sino que también muestra altos valores, en función del tiempo, de reposición de una falla cualquier en la red.

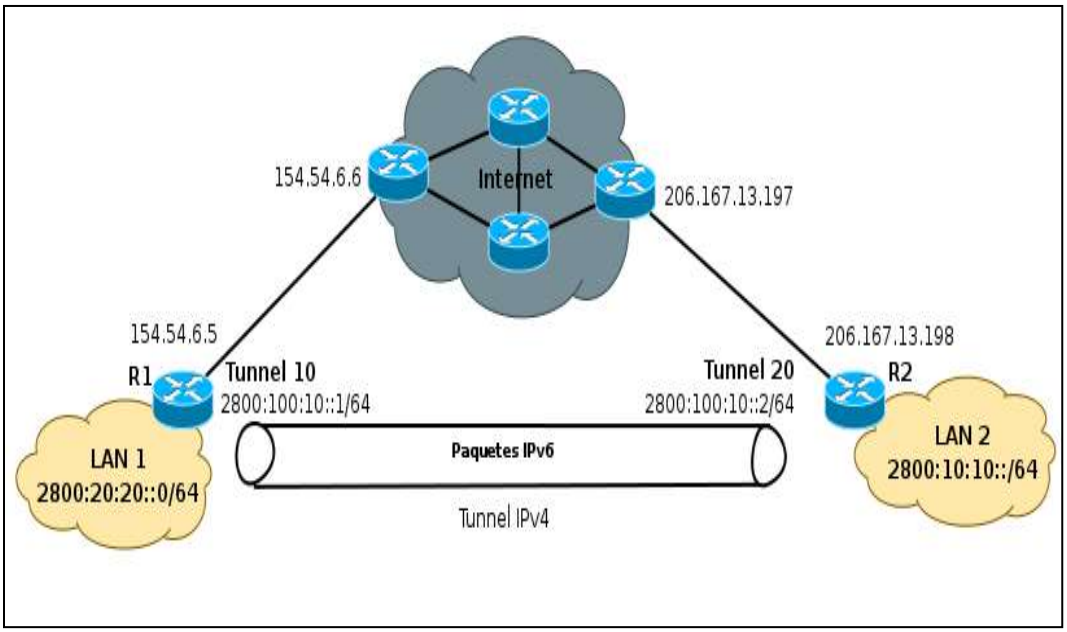
- Túneles automáticos: estos no requieren de una configuración estática en ambos extremos sino que se establecen automáticamente con una configuración mínima, lo cual permite entre otras cosas, simplificar la operación y mantenimiento de la red y promete mejor tiempos de convergencia.

3.3.1. Túneles configurados

Esta opción requiere la configuración manual de los puntos finales del túnel. En este, las direcciones IPv4 de los puntos finales del túnel no derivan de direcciones dentro de las direcciones IPv6 origen y destino o de las direcciones del siguiente salto de la ruta correspondiente.

Típicamente, las configuraciones de túnel entre los enrutadores se configuran manualmente. La configuración de la interfaz del túnel consiste en las direcciones IPv4 de los puntos finales del túnel, las cuales deben de ser configuradas manualmente junto con las rutas estáticas que usa la interfaz del túnel, ver figura 21.

Figura 21. **Ejemplo de túneles configurados (manuales)**



Fuente: elaboración propia.

3.3.2. Túneles automáticos

Es un túnel que no requiere configuración manual, en los puntos finales del túnel se determinan por el uso de las interfaces lógicas, las rutas y las direcciones IPv6 origen y destino.

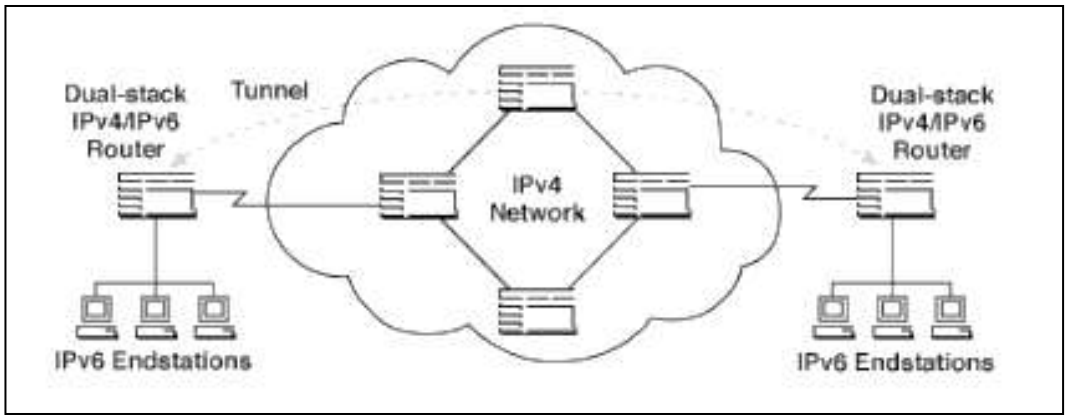
Dentro de este grupo se pueden diferenciar tres clases:

- Túneles automáticos 6to4
- Túneles automáticos Teredo
- Túneles automáticos IPv6 *Rapid-Deployment* (6RD)

Las primeras dos clases tienen un factor común y es que utilizan el prefijo 2002::/16, un prefijo definido por la IANA para túneles IPv4 – Ipv6.

6RD, que es una extensión de los túneles 6to4 tiene varias diferencias, como el que no emplea el prefijo 2002::/16 y otra diferencias que obligan a tratarlo con una clase aparte y no únicamente como una extensión de los túneles automáticos 6to4.

Figura 22. **Ejemplo de túneles automáticos**



Fuente: elaboración propia.

3.3.2.1. Túneles automáticos 6to4

6to4 es una asignación de direcciones y tecnología de túneles automáticos de enrutador a enrutador que se utiliza para proveer conectividad unicast IPv6 entre sitio IPv6 y equipos a través de la Internet IPv4.

6to4utiliza el prefijo de direccionamiento global:

2002:WWXX:YYZZ:: / 48

En el cual WWXX:YYZZ es la representación hexadecimal de una dirección IPv4 pública (w.x.y.z) asignada a un sitio o equipo. La dirección completa 6to4 es:

2002:WWXX:YYZZ:Subnet ID:Interface ID

6to4se describe en el RFC 3056, el cual define los siguientes términos:

- Host6to4. Cualquier hostIPv6 que se configura con por lo menos una dirección 6to4 (una dirección global con el prefijo 2002::/16). Los *hosts* 6to4no requieren ninguna configuración manual y crean direcciones 6to4usando mecanismos de autoconfiguración de direcciones estándar.

- Enrutador 6to4. Un enrutador IPv6/IPv4 que soporta el uso de interfaces de túnel 6to4 y es usada típicamente para reenviar tráfico de direcciones 6to4 entre los *hosts* 6to4. Los enrutadores 6to4 requieren procesamiento adicional lógico para el correcto encapsulado y decapsulado y pueden requerir configuración manual adicional.

Dentro de un sitio, los enrutadores IPv6 locales promocionan prefijos 2002:WWXX:YYZZ:SubnetID::/64 para que los *hosts* puedan crear una dirección 6to4 autoconfigurado y rutas de prefijo de 64 bits que se usan para entregar tráfico entre hosts 6to4dentro del mismo sitio.

Los hosts en las redes individuales son configurados automáticamente con rutas de subred de 64 bits para entrega directa a vecinos y una de *default* con la dirección de siguiente salto del enrutador que hace la promoción, todo el tráfico IPv6 que no coincide con un prefijo de 64 bits usado por una de las subredes dentro del sitio se reenvían a un enrutador 6to4 en la frontera del sitio.

Cuando se usan *host* 6to4, en la infraestructura de ruteo de IPv6 dentro de un sitio, el enrutador 6to4 en la frontera del sitio, y un enrutador de relay 6to4, se pueden realizar los siguientes tipos de comunicaciones:

- Un *host*6to4se puede comunicar con otro host 6to4 dentro del mismo sitio. Este tipo de comunicación está disponible usando la infraestructura de ruteo de IPv6, la cual provee alcance a todos los *hosts* dentro del sitio.

- Un cic 6to4 se puede comunicar con los *host* 6to4 en otros sitios a través de la internet IPv4. Este tipo de comunicación ocurre cuando los *hosts* 6to4 en reenvían tráfico IPv6 con destino a un *host* 6to4 en otro sitio al enrutador 6to4 del sitio local. El enrutador 6to4 del sitio local envía por el túnel el tráfico IPv6 hacia el enrutador 6to4 del sitio destino en la internet IPv4. El enrutador 6to4 en el sitio destino quita el encabezado IPv4 y reenvía el paquete IPv6 al *host* 6to4 apropiado usando la infraestructura de ruteo IPv6 en el sitio destino.

- Un *host* 6to4 se puede comunicar con *host* en la internet IPv6. Este tipo de comunicación pasa cuando un *host* 6to4 reenvía tráfico IPv6 el cual su destino es un *host* en la InternetIPv6 al enrutador 6to4 del sitio local. El enrutador 6to4 del sitio local envía por el túnel el tráfico IPv6 a un enrutador de relay 6to4, el cual está conectado a ambas redes, la internet IPv4 y la Internet IPv6. El enrutador de relay 6to4 quita los encabezados IPv4 y reenvía el paquete IPv6 al *host* de la internet IPv6 apropiado usando la infraestructura de ruteo de la Internet IPv6.

Todos estos tipos de comunicación usan el tráfico IPv6 sin los requerimientos de obtener tanto una conexión directa a la Internet IPv6 como un prefijo de dirección IPv6 global de un proveedor de servicios de internet.

3.3.2.2. Túneles automáticos Teredo

Teredo es una tecnología de transición que proporciona conectividad IPv6 a *hosts* que soportan IPv6 pero que se encuentran conectados a internet mediante una red IPv4. Comparado con otros protocolos similares, la característica que lo distingue es que tiene la capacidad de realizar su función incluso detrás de dispositivos NAT, como los enrutadores domésticos.

Teredo opera usando un protocolo de túneles independiente de la plataforma diseñado para proporcionar conectividad IPv6 encapsulando los datagramas IPv6 dentro de datagramas UDP IPv4. Estos datagramas pueden ser encaminados en Internet IPv4 y a través de dispositivos NAT. Otros nodos Teredo, también llamados Teredo relays, que tienen acceso a la red IPv6, reciben los paquetes, los desencapsulan y los direccionan.

Teredo está diseñado como una tecnología de transición con el objetivo de ser una medida temporal. En el largo plazo, todos los hosts IPv6 deberían usar la conectividad IPv6 nativa y desactivar Teredo cuando la conectividad IPv6 esté disponible.

El protocolo de túneles IPv6 sobre IPv4 más común, 6to4, requiere que el final del túnel tenga una dirección IPv4 pública. Sin embargo, actualmente muchos hosts se conectan a Internet IPv4 a través de uno o varios dispositivos NAT, por lo general por el agotamiento de las direcciones IPv4. En esta situación, la única dirección IPv4 pública se asigna al dispositivo NAT y es necesario que el protocolo 6to4 esté implementado en este dispositivo. Muchos de los dispositivos NAT usados actualmente no pueden ser actualizados para implementar 6to4 por razones técnicas o económicas.

Teredo soluciona este problema encapsulando paquetes IPv6 dentro de datagramas UDP IPv4, los cuales pueden ser reenviados correctamente por NATs. Por lo tanto los hosts IPv6 que se encuentran detrás de dispositivos NAT pueden usar los túneles Teredo incluso si no disponen de una dirección IPv4 pública. Un *host* que implemente Teredo puede tener conectividad IPv6 sin cooperación por parte de la red local o del dispositivo NAT.

El protocolo Teredo incluye una disposición para el proceso de extinción del protocolo: una implementación Teredo debería proporcionar una forma para dejar de usar la conectividad Teredo cuando IPv6 haya madurado y la conectividad esté disponible usando un mecanismo menos frágil.

3.3.3. 6RD

Esta técnica se utiliza para comunicar islas IPv6 a través de un núcleo de IPv4, mediante el uso de encapsulación de IPv6 sobre IPv4. Es muy similar a la técnica de túnel automático 6to4, con dos grandes diferencias:

- 6RD no requiere de direcciones cuyo prefijo sea 2002 :: / 16, por lo tanto, el prefijo puede ser del bloque de direcciones que administra el propio proveedor de servicio. Esta función permite que el dominio operativo de 6RD este dentro de la misma red del proveedor de servicio. Desde el punto de vista del cliente y de Internet en general basado en IPv6 conectado a una red habilitada para 6RD al proveedor de servicio, el servicio proporcionado es equivalente a IPv6 nativas.

- Los 32 bits del IPv4 de destino no necesita ser transportados en la cabecera de carga útil IPv6. El destino de IPv4 se obtiene a partir de una combinación de bits en la cabecera de carga útil y la información en el enrutador. Además, la dirección IPv4 no está en una ubicación fija en la cabecera IPv6 como lo es en 6a4.

En túneles automáticos 6to4, los túneles determinan la dirección de destino adecuado mediante la combinación del prefijo IPv6 con direcciones IPv4 únicas del enrutador destino comenzando con el prefijo 2002 :: / 16, en este formato:

2002:border-router-IPv4-address::/48

Este método deja otros 16 bits del prefijo de 64 bits para numerar redes en un sitio determinado. Y todas las direcciones de interfaz dentro del enrutador

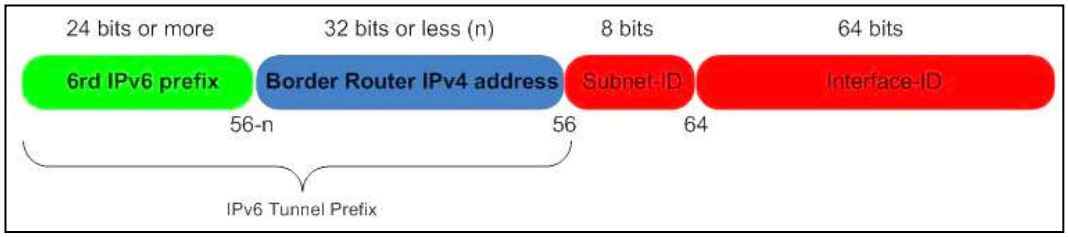
frontera debe comenzar con este mismo 2002: frontera-router-IPv4-prefijo de la dirección con el fin de ser capaz de comunicarse a través del túnel 6to4 automático.

Además de la configuración básica del túnel, proporcionar algún encaminamiento de los paquetes deseados a través del túnel también es necesario. Esto se realiza normalmente utilizando una ruta estática (la configuración más sencilla). Por ejemplo, para encaminar los paquetes destinados para el prefijo 2002 :: / 16 sobre la interfaz de túnel tunnel0 6a4, se podría configurar la siguiente ruta estática (la sintaxis del comando puede variar en los distintos modelos de enrutadores en el mercado):

ipv6 route 2002::/16 tunnel 0

Con 6RD, los proveedores de servicio pueden usar su prefijo asignado por ellos mismos en lugar de utilizar 2002 para la construcción del túnel. De esta cuenta la dirección del túnel no inicia con el prefijo 2002 sino más bien con el prefijo asignado por el ISP.

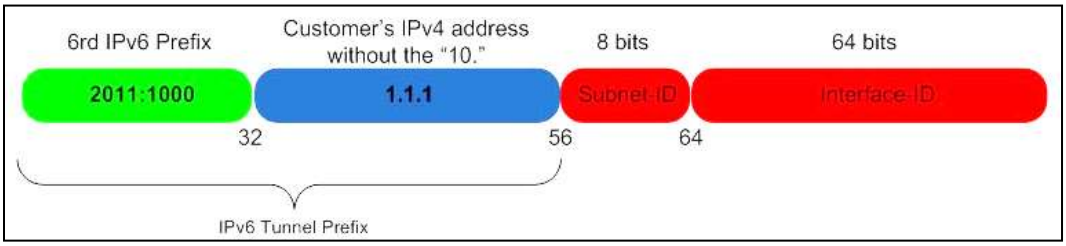
Figura 23. **Campos de dirección 6RD**



Fuente: elaboración propia.

Y aún más, con 6RD existe la posibilidad de agrupar los bits en el campo de la dirección del enrutador fronterizo. Imaginemos que el ISP usa el rango 10.0.0.0 / 8 para hacer frente a todas sus *loopbacks* en el enrutador. Por lo tanto, si el destino del túnel es un enrutador en el mismo dominio, el primer octeto de la dirección IPv4 no añade ninguna información adicional. En este caso, 6RD da la posibilidad de reducir esta primer octeto, y añadiendo a la dirección de túnel solamente los tres últimos octetos de la dirección IPv4. Como ejemplo vea la figura 24:

Figura 24. **Campos de dirección 6RD**



Fuente: elaboración propia.

4. ANÁLISIS DE TÉCNICA BASADA EN TÚNELES DE IPV4

En este capítulo se considerará la implementación de túneles IPv4 como técnica de transición de IPv4 a IPv6 dentro de la red de un ISP. Con este análisis se podrán identificar las ventajas y desventajas de esta técnica así como las premisas de diseño a considerar para lograr optimizar aspectos técnicos y económicos al momento de implementarla.

En la actualidad, cada ISP tiene desplegada una red IPv4 que no necesariamente es igual a la de otro ISP, al contrario, difícilmente entre ISP se logren encontrar redes similares en función de equipos y topologías físicas pero a nivel lógico, se puede encontrar similitudes en las funciones que corren los distintos elementos de red por lo que la idea será partir de una red tipo que contemple a nivel físico y lógico varios de los aspectos comunes que se esperan encontrar.

La red que se empleará para el análisis se dividirá en cuatro grupos: Acceso, Distribución, Core y Edge. En cada una de las redes ISP se debe tener estos cuatro grupos bien identificados (esto es una buena práctica de diseño).

El acceso hace mención a todos los equipos donde se conectan los equipos terminales. Comúnmente este grupo lo conforman equipos que operan en la capa 2 de OSI, es decir, switches; aunque la tendencia de las nuevas redes convergentes apunta a crecer la capa 3 de OSI a este grupo, especialmente por los altos tiempos de convergencia que LTE demanda.

Los grupos de distribución son puntos de agregación y terminación de anillos o buses de acceso donde también se finalizan los dominios de *broadcast*. En otras palabras, la distribución es el grupo de equipos frontera donde termina la capa 2 e inicia la capa 3. Adicionalmente, es aquí donde la red MPLS tiene su frontera en los equipos PE (*Provider Edge*)

El grupo Core son equipos que únicamente corren MPLS, aquí no existe conmutación por direcciones IP sino únicamente por etiquetas MPLS. Son equipos robustos con anchos de banda altos.

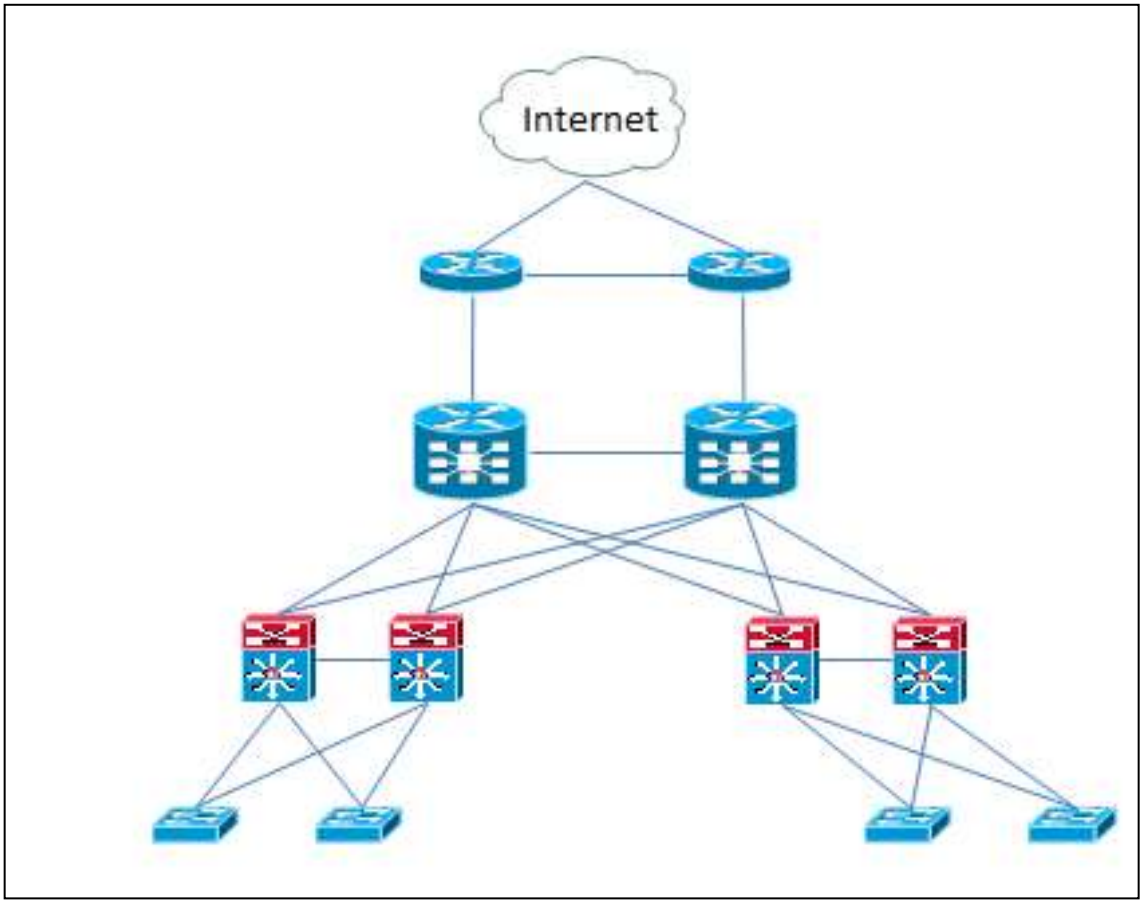
Por último está el grupo Edge, que son los equipos frontera de un ISP, normalmente, los equipos frontera de un sistema autónomo (en términos de BGP). Aquí normalmente es dónde se conectan otros ISP y proveedores de Internet.

Tabla XI. **Descripción de capas, función, equipos y vendors**

Capa	Función	Equipo	Vendor
Acceso	Conmutación a nivel L2. Los equipos en esta capa son encargados de manejar las distintas VLANs. La conmutación la hacen en función de dirección MAC.	Switch	Cisco / Huawei
Distribución	Terminación dominios L2 (Gateways), Conmutación L2 y L3. Estos equipos son encargados de terminar los dominios de brodcast, los encargados de insertar o remover etiquetas MPLS.	Switch L3	Cisco / Huawei
Core	Conmutación por etiquetas (MPLS). Estos equipos no hacen otra cosa mas que transporte, a estos equipos no se conectan clientes, todo el tráfico aquí va etiquetado.	Router	Cisco / Juniper
Edge	Frontera AS del ISP, Conexión a otros ISP e Internet. Estos equipos son los demarcadores entre un sistema autónomo y otro como lo pueden ser otros proveedores de servicio o proveedores de internet	Router	Cisco / Juniper

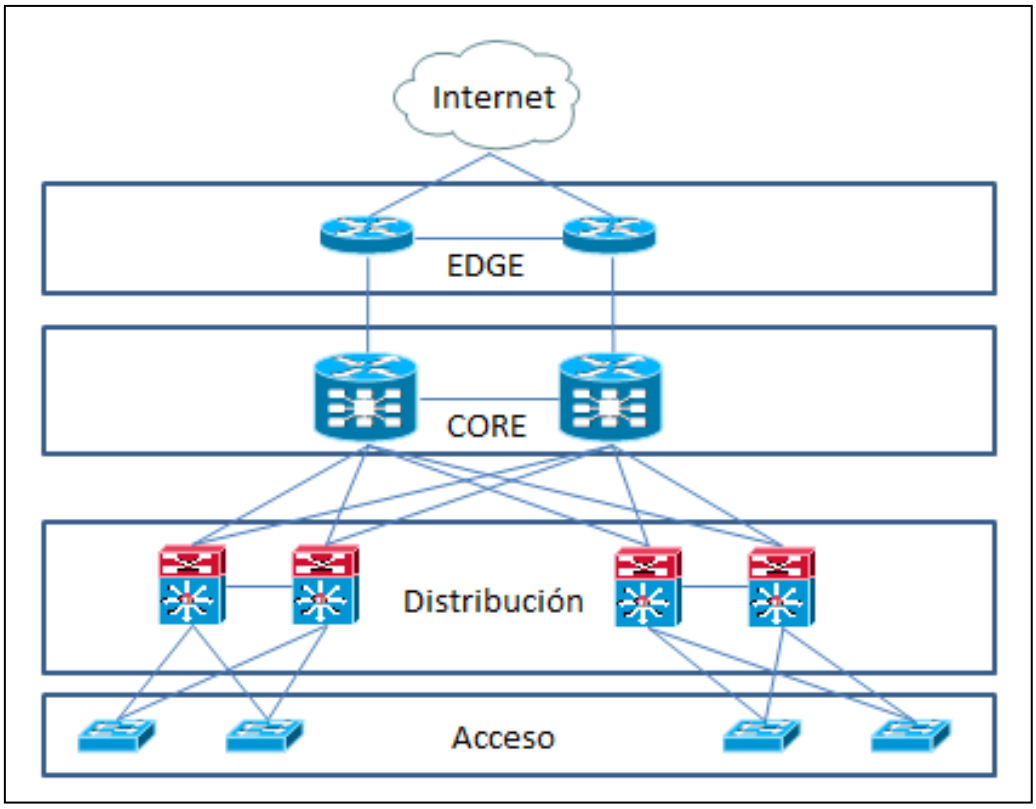
Fuente: elaboración propia.

Figura 25. **Topología física a analizar**



Fuente: elaboración propia con programa, Adobe Illustrator.

Figura 26. **Identificación de capas en topología física**



Fuente: elaboración propia, con programa Adobe Illustrator.

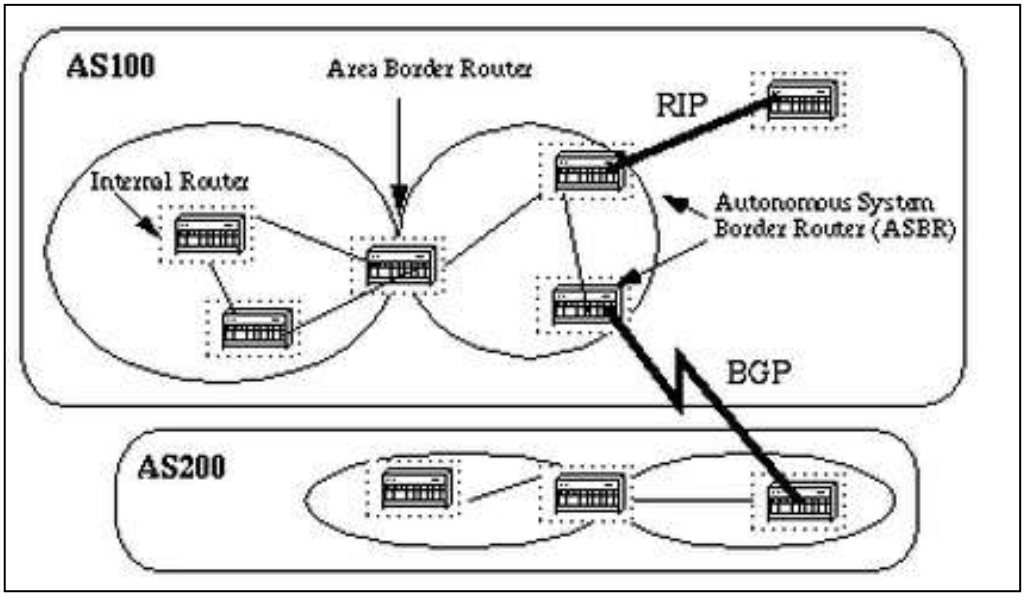
A nivel lógico se va considerar como IGP el protocolo de ruteo OSPFv2 que es lo más común de encontrar entre ISP. Para el EGP se utiliza BGP por ser el único protocolo de ruteo definido para esta función al día de hoy. Dentro del IGP se maneja una arquitectura modelo de OSPFv2 con un área 0 que conecte los equipos CORE, EDGE y Distribución. Los equipos de distribución, a su vez, interconectan a áreas distintas conectadas al área 0 funcionando como ABR (*Area Border Router*) y los EDGE como ASBR (*Autonomous System Boundary Router).*

Un enrutador ABR se define como un enrutador que pertenece a múltiples áreas de OSPF y los conecta a su vez con el área 0, llamada también el área backbone.

Un enrutador ASBR se define como un enrutador que funciona como gateway o redistribuidor entre OSPF y otro protocolo de ruteo (IGRP, EIGRP, IS-IS, RIP, BGP, estático).

La figura 27 ejemplifica la diferencia entre un ABR y un ASBR

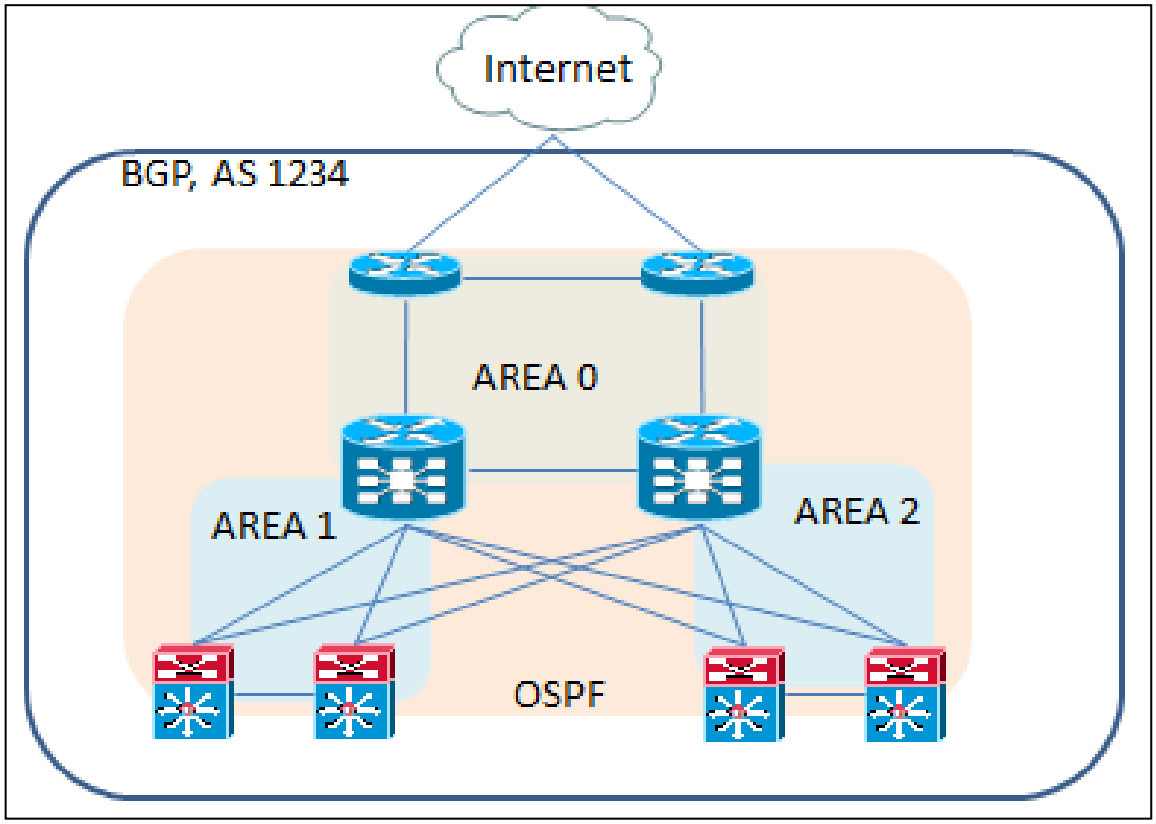
Figura 27. **Diferencia entre un ABR y un ASBR**



Fuente: www.cisco.com/c/en/us/support/ /ip/open-shortest-path-first-ospf/7039-1.html. Consulta: 1 febrero de 2014.

El diagrama lógico queda como se muestra en la figura 28.

Figura 28. **Diagrama lógico áreas OSPF**



Fuente: elaboración propia, con programa Adobe Illustrator.

4.1. Arquitectura y diseño de túneles dentro de un ISP

Para poder definir la arquitectura y diseño de los túneles dentro de un ISP, previamente se debe definir y acotar los servicios que se desean dar a los usuarios finales.

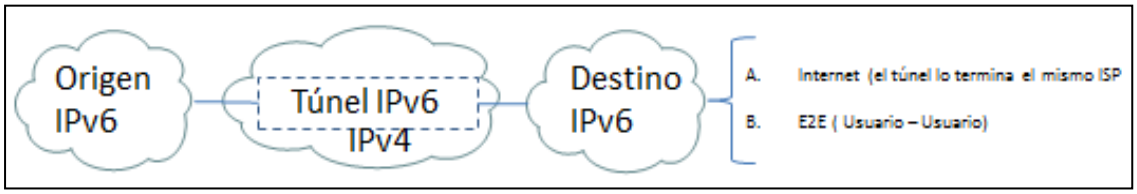
Cuando se piensa en IPv6 existen dos tipos de necesidades que un usuario puede requerir:

- Enlaces internet IPv6: comunicación IPv6 entre un cliente e internet.

- Enlaces corporativos IPv6: comunicación IPv6 entre dos o más sitios que conforman la empresa.

En los enlaces de internet IPv6 debe ser mandatorio que el contenido en internet sea IPv6, esto es que los servidores de contenido (Facebook, Youtube, Actualizaciones de Microsoft, itunes, por poner algunos ejemplos) soporten IPv6.

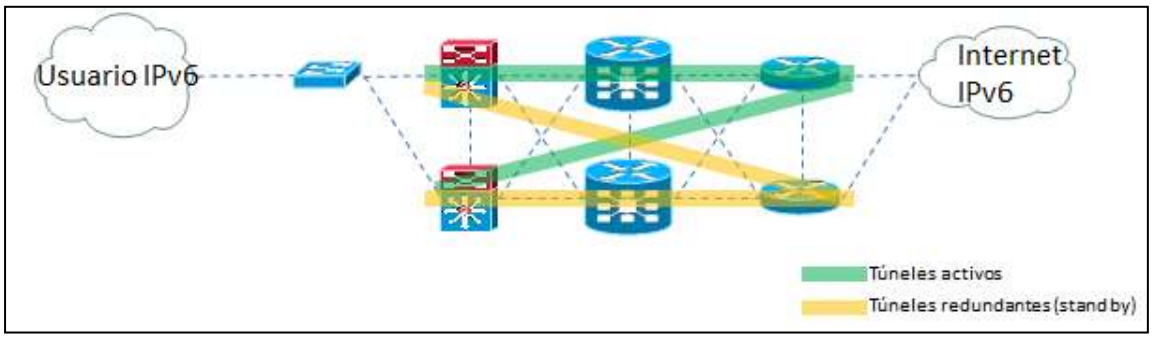
Figura 29. **Requerimientos tipo de los usuarios**



Fuente: elaboración propia, con programa Adobe Illustrator.

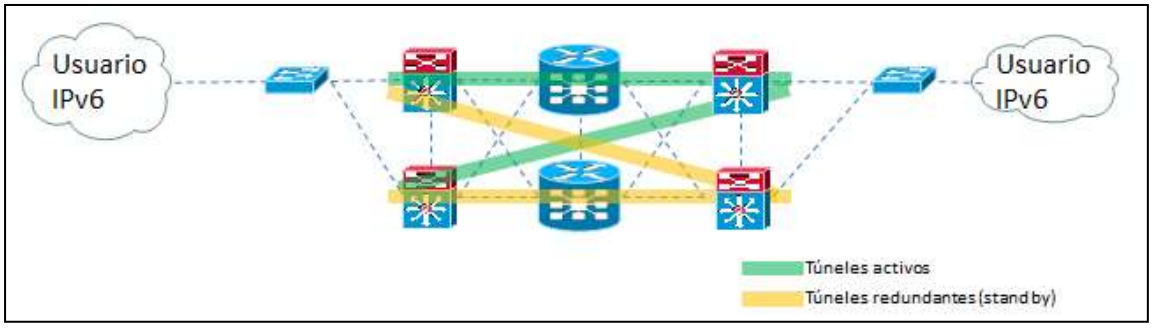
Dado lo anterior, se tienen las siguientes arquitecturas, las cuales que cumplen con lo requerido por parte del usuario final.

Figura 30. **Servicio Internet IPv6**



Fuente: elaboración propia, con programa Adobe Illustrator.

Figura 31. **Servicio E2E IPv6**

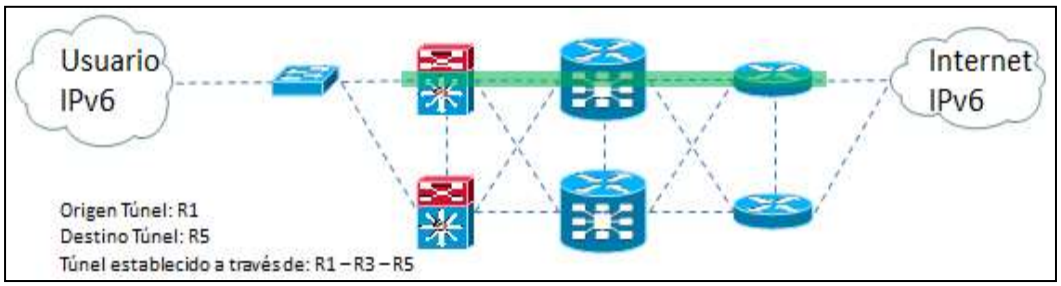


Fuente: elaboración propia, con programa Adobe Illustrator.

La recomendación, como se puede observar en las figuras 32 y 33, es levantar túneles 1+1 (redundantes) que permitan los escenarios de falla que se describen a continuación.

En caso que la red no presente fallas a nivel de equipo o enlace, el túnel deberá formarse se la forma que indica la figura 32.

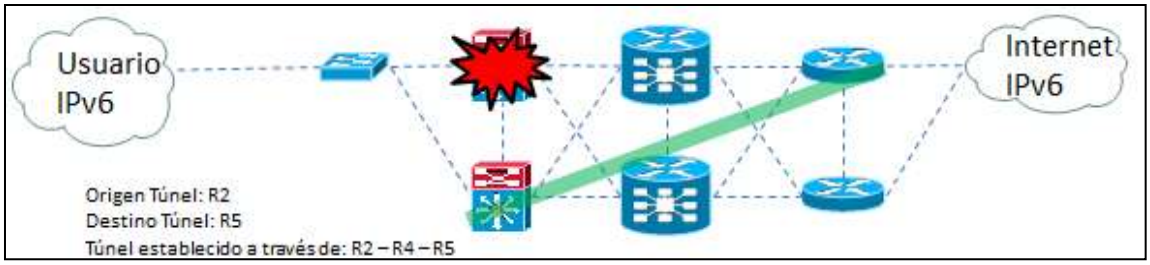
Figura 32. **Túnel IPv4 – IPv6, escenario normal**



Fuente: elaboración propia, con programa Adobe Illustrator.

El primer escenario de falla que se indica en la figura 33 sería que el equipo R1 falle, ya sea la tarjeta de línea dónde se conecta el cliente o las supervisoras presenten alguna falla que traiga abajo el equipo. Otra posibilidad es una falla de energía en todo el edificio, en este caso el túnel deja de ser establecido por R1 y el tráfico es conmutado al que establece R2. Es necesario indicar que en realidad el túnel que establece R2 siempre está establecido al mismo tiempo que el que establece R1, la conmutación en este caso la lleva acabo el protocolo HSRP (L2).

Figura 33. **Escenario de falla A**

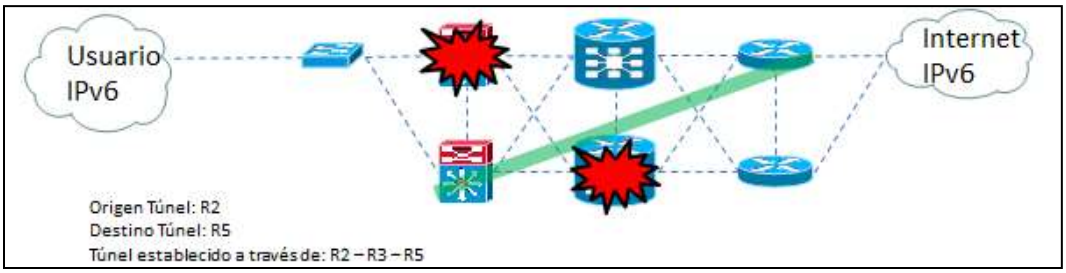


Fuente: elaboración propia, con programa Adobe Illustrator.

En redes de ISP grandes es muy común ver dos fallas simultáneas por lo que se hace necesario considerar ambas situaciones y analizar, considerar o documentar el comportamiento de la red. Para este caso, el escenario es en el que R1 y R4 queden fuera ya sea por problemas propios de hardware o cortes de fibra.

En el caso de R1, nuevamente HSRP se encarga de conmutar el tráfico a R2. En el caso de R4. La configuración de OSPF en los enrutadores debe ser la correcta y no debe ser alterada para asegurar que las rutas del siguiente salto existan a manera que sea OSFP el que se encarga de buscar otra ruta para establecer el túnel. De esta manera se garantiza la continuidad del servicio.

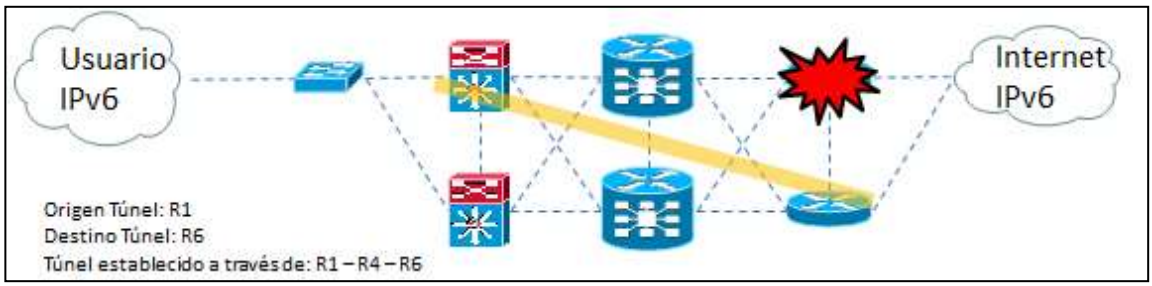
Figura 34. **Escenario de falla B**



Fuente: elaboración propia, con programa Adobe Illustrator.

El escenario 3 plantea la falla en uno de los equipos de borde (ver figura 37). En estos casos, el equipo que establece el túnel detecta que el destino del mismo tiene problemas y el establece el túnel de *back-up* que manualmente se ha predefinido en el equipo.

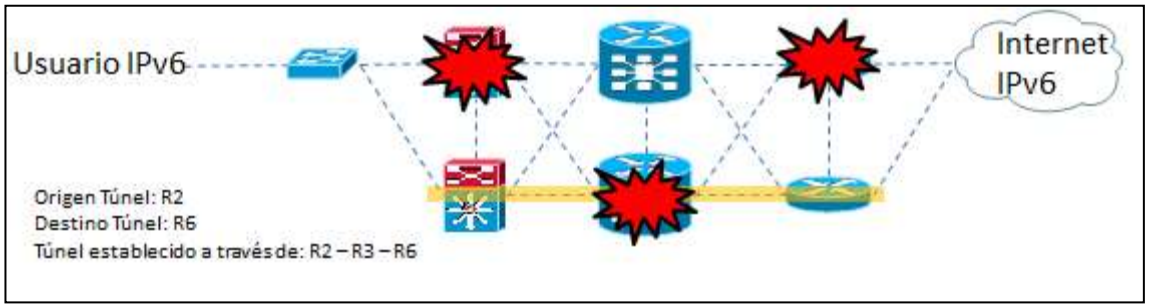
Figura 35. **Escenario de falla C**



Fuente: elaboración propia, con programa Adobe Illustrator.

En el escenario 4 se considera el peor de los casos que la arquitectura puede soportar, que serían 3 fallas simultáneas (ver figura 38), en este caso se hace uso de los tres protocolos de protección al mismo tiempo: HSRP, convergencia de OSPF y túnel *back-up* en el equipo que establece el túnel. En base a esto se puede concluir que la arquitectura propuesta es bastante robusta.

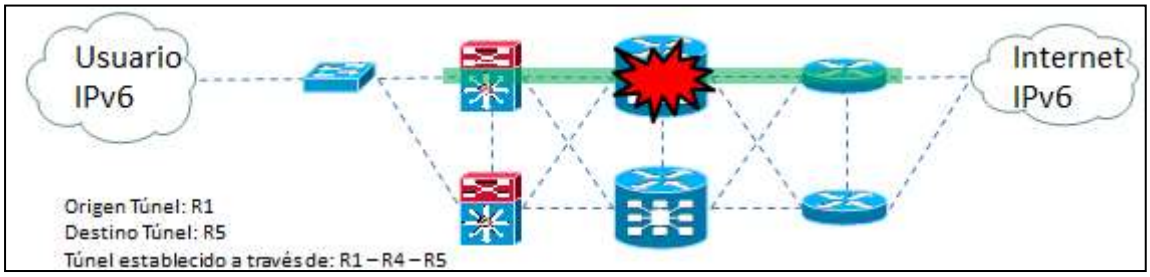
Figura 36. **Escenario de falla D**



Fuente: elaboración propia, con programa Adobe Illustrator.

El escenario 5 requiere de una convergencia a nivel del IGP (ver figura 39). Este escenario, es posible gracias al tipo de cableado que se ha realizado entre los equipos.

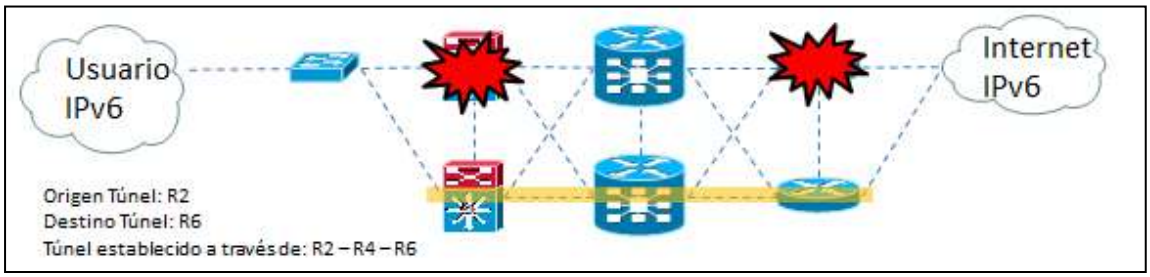
Figura 37. **Escenario de falla E**



Fuente: elaboración propia, con programa Adobe Illustrator.

En el escenario 6 se consideran dos fallas simultáneas (ver figura 37). Aquí debe converger HSRP del lado del cliente, y se debe establecer el túnel *back-up.*

Figura 38. **Escenario de falla F**



Fuente: elaboración propia, con programa Adobe Illustrator.

Se muestra en resumen de como a nivel de OSPF túneles activos y/o redundantes son establecido o reestablecidos según sea el caso:

Tabla XII. **Descripción de capas, función, equipos y vendors**

Escenarios	Origen Túnel	Destino Túnel	*Path* para establecer el túnel		
Normal	R1	R5	R1	R3	R5
De falla A	R2	R5	R2	R4	R5
De falla B	R2	R5	R2	R3	R5
De falla E	R1	R5	R1	R4	R5
De falla C	R1	R6	R1	R4	R6
De falla F	R2	R6	R2	R4	R6
De falla D	R2	R6	R2	R3	R6

Fuente: elaboración propia, con programa Microsoft Excel 2010.

4.2. Temas a considerar para la implementación de túneles de IPv4

Deben considerarse varios temas para la implementación de túneles IPv4, ya que como cualquier protocolo presenta ventajas y desventajas en su aplicación, asimismo presenta diversas premisas que deben ser tomadas en cuenta.

4.2.1. Impacto en migraciones

Al momento de analizar el impacto que la migración de IPv4 a IPv6 haciendo uso de túneles (configurados y/o automáticos), como técnica de transición en una red IPv4 en producción se deben considerar los siguientes escenarios válidos y aplicables a cualquier red:

- El 100 por ciento de la red IPv4 está lista para soportar IPv6 y habilitación de túneles (lo que inglés se denomina IPv6 Ready).

- La red IPv4 parcialmente está lista para soportar IPv6 y habilitación de túneles.

    - Las tarjetas de línea no soportan IPv6 o la habilitación de túneles.
    - Las supervisoras no soportan IPv6 o la habilitación de túneles.
    - Una combinación de los dos incisos anteriores.

- Que el 100 por ciento de la red IPv4 no esté lista para soportar IPv6 y habilitación de túneles.

Aunque en los puntos anteriores se menciona el hecho de que debe existir la capacidad de poder crear túneles (punto mandatorio para poder trabajar en una transición IPv4 a IPv6 por medio de esta técnica), la realidad es que debido a que los túneles se habilitan en redes IPv4 y es una tecnología ampliamente utilizada para otros fines en redes actuales lo más seguro es que una red IPv4 actual ya los soporta por lo que aunque si es un punto crítico que se debe tomar en cuenta no deberá preocupar al encargado de la implementación.

Adicionalmente, se debe considerar en paralelo los siguientes escenarios:

- El cliente desea migrar IPv4 a IPv6 en su totalidad.

- El cliente desea mantener dos redes en paralelo (IPv4 para unos servicios e IPv6 para otros).

4.2.1.1. Actualización de tarjetas controladas

Al momento de planificar una actualización de tarjetas controladoras en equipos de red en producción, se deben considerar el modelo/proveedor del equipo y los equipos categorizados como Carrier Class. Los cuales se describen a continuación.

- Dependiendo del modelo/proveedor del equipo, existe la posibilidad de que se requiera de un reinicio completo del equipo a la hora de instalar las nuevas tarjetas controladoras para que reconozca todo el Hardware. Esto implica que todos los servicios albergados en este estén propensos a ser interrumpidos durante un lapso de tiempo que puede rondar desde los 5 hasta los 20 minutos.

- En la actualidad, los equipos categorizados como Carrier Class, tienen la bondad de que, a manera de no interrumpir el servicio, permite al implementador, bajo un procedimiento específico, la manera en que no se deba reiniciar la totalidad del equipo al momento de realizar la actualización. Lógicamente para que esto sea viable, el equipo debe de contar con un esquema de tarjetas controladoras N+1. Sin embargo, y aun en estos casos, existe la posibilidad de que un reinicio sea requerido por el equipo debido a alguna falla que presente el equipo durante el proceso.

4.2.1.2. Instalación de tarjetas en línea

Si bien la instalación de tarjetas de líneas es un procedimiento que no requiere reinicio del equipo la mayoría de casos se deben tomar en consideración los siguientes aspectos:

- Se debe validar que el sistema operativo actual en el equipo sea compatible con las nuevas tarjetas.

- En caso de que todos los *slots* del equipo se encuentren ocupados y siempre que la ocupación de puertos lo permita, se deberá migrar servicios entre las tarjetas actuales para liberar un slot donde se instalará la nueva tarjeta. Esta migración previa de puertos conlleva una baja en los servicios específicos que vayan en dichos puertos. Normalmente, como estamos en los equipos PE, estos puertos difícilmente están dedicados para un cliente en especial sino más bien aquí están conectados *switches* de acceso por lo que una baja en un puerto en el PE representa la baja de al menos 24 puertos en el acceso sino es que más. (esto depende de cómo el ISP tiene diseñada su red de acceso)

En caso de que el sistema operativo no sea compatible con las nuevas tarjetas se deberá actualizar en sistema operativo, esto implica un chequeo en la memoria flash y RAM del equipo para ver que se tenga la capacidad mínima requerida por el nuevo sistema operativo. Adicional, y dependiendo del modelo/proveedor, la actualización puede requerir de un reinicio en el equipo.

Tabla XIII. **Niveles de impacto para habilitar túneles IPv6**

Actividad	Impacto	Observaciones
Cambio de supervisoras	Alto	Requiere un reinicio en el equipo completo
Instalación tarjetas de línea	Bajo	Se debe validar que el sistema operativo actual soporta la tarjeta
Migración clientes entre tarjetas de línea	Medio	Baja del servicio en el/los cliente/clientes a migrar.
Habilitar túneles IPv4 - IPv6	Bajo	Habilitación de túneles bajo demanda
Actualización de sistema operativo	Alto	Dependiendo del modelo/vendor, algunos requieren reinicio completo del equipo

Fuente: elaboración propia, con programa Microsoft Excel 2010.

4.2.2. Tiempos de convergencia

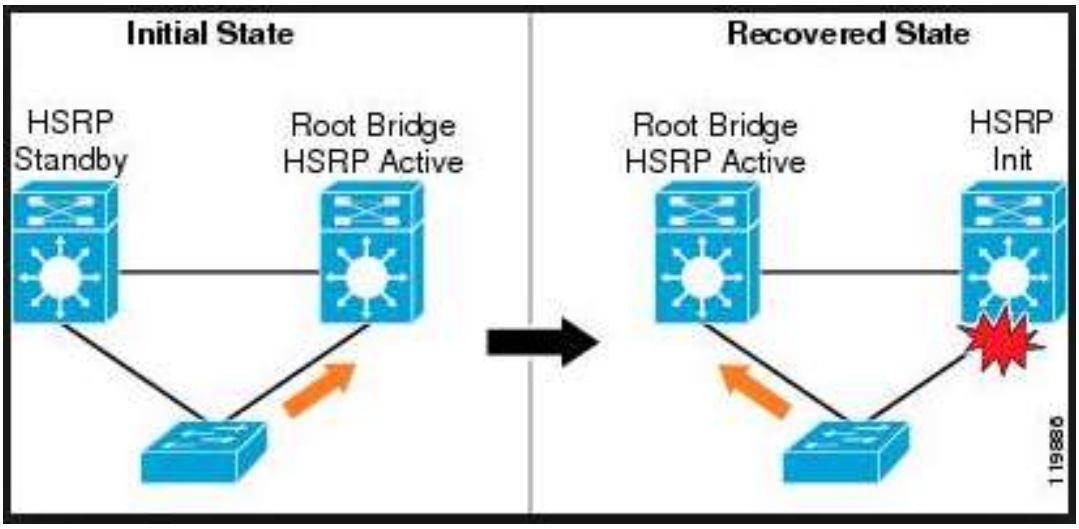
En el diseño analizado se observa que algunas fallas activan uno o más mecanismos de protección a nivel L2 o L3 dependiendo del tipo de falla. El objetivo es lograr identificar los tiempos de convergencia de cada uno por separado y en conjunto.

4.2.2.1. HSRP (Hot Stand-by Router Protocol)

Este protocolo se origina por la necesidad de brindar una protección a nivel de Gateway en una LAN.

El funcionamiento del mismo se muestra en la figura 38:

Figura 39. **Funcionamiento HSRP**



Fuente:http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html. Consulta 15 de febrero de 2014.

El protocolo crea una IP virtual entre los dos enrutadores, la misma es situada en el equipo definido por el administrador de los equipos como primario, y cuando este tiene una falla o existe una falla en el enlace, el protocolo se encarga de deshabilitar la IP virtual en el enrutador activo y de activarla en el enrutador pasivo. Del punto de vista del operador de red es como si la IP virtual "flota" de un equipo a otro. Con esto se logra brindar un esquema de protección sin la necesidad de que el usuario final deba cambiar la IP del *gateway*, para el usuario final esto es transparente.

Bajo el diseño analizado, se reemplaza la palabra *gateway* por el enrutador que tiene el túnel IPv4-IPv6 activo primario (enrutador activo en HSRP) y el que tiene el túnel IPv4-IPv6 activo secundario (enrutador pasivo en HSRP)

Para configurar HSRP se requiere del entendimiento de muchos parámetros y logística que sigue el protocolo que está fuera del alcance de este documento, para efectos del análisis que se está realizando es suficiente indicar el parámetro que hace referencia a los tiempos de convergencia del mismo.

4.2.2.2. Paquetes *Hello*

Los paquetes hello son los encargados de estar censando el enlace L2 entre los dos enrutadores. Por *default*, este valor está seteado a 3 segundos, es decir que cada 3 segundos los enrutadores se hablan para saber que están allí.

Este valor puede ser modificado manualmente por el operador, sin embargo es de tomar en cuenta que un valor muy bajo impacta directamente en la carga del CPU de los equipos, ya que el mismo los interpreta como interrupciones de alta prioridad. La recomendación es configurarlos en valores mayores a 4 segundos, siendo 5 un valor recomendado.

4.2.2.3. Paquete Hold Time

Paquete que determina cuántos segundos debe esperar por un paquete *hello* antes de dar por perdido el enlace/enrutador activo y habilitar la IP virtual en el enrutador redundante.

Este valor por default es de 10 segundos, el mismo puede ser modificado por el operador pero se recomienda que el mismo no sea menor a 3 veces el tiempo definido para los paquetes *hello*. La razón es sencilla, se debe impedir el efecto de *flapping* en las interfaces. El valor recomendado es de 15 segundos.

Este parámetro es el que determinar el tiempo de convergencia, que bajo las mejor prácticas sería de 15 segundos luego de que se ha originado la falla.

4.2.2.4. OSPF (Open Short Path First)

Es un protocolo de ruteo dinámico cuyo objetivo principal es el de anunciar redes dentro de un AS de manera dinámica sin intervención humana. Para lograr esto, trabaja bajo varios algoritmos, siendo el algoritmo de Dijkstra la base. Este algoritmo (como del funcionamiento de OSFP) está fuera del alcance de este documento, solo se pone énfasis a los tiempos de *hello* y *hold* antes de dar por caído un vecino.

En OSPF, el tiempo de *Hello* recomendado es de 10 segundos, y el de *Hold (Deadtime*) debe ser 4 veces mayor por recomendación de diseño del protocolo, esto para evitar efectos debidos a *flapping* de las interfaces.

El tiempo de convergencia luego de una falla es de 40 segundos.

4.2.2.5. Tiempos de convergencia de los túneles

Los túneles automáticos activos y *stand-by* están presentes en el *Control Plane* de los enrutadores por lo que el tiempo de convergencia es simultáneo.

En caso de los túneles manuales, depende de los tiempos de respuesta del equipo de soporte a la red (NOC).

Tabla XIV. **Tiempos de convergencia**

Escenarios de falla	Protocolos utilizados	Tiempo de convergencia esperado
1	HSRP	15 Segundos
5	OSPF	40 Segundos
2	HSRP + OSPF	40 Segundos
3	Túnel Back Up	Inmediato
6	HSRP + Túnel Back Up	15 Segundos
4	HSRP + OSPF + Túnel Back Up	40 Segundos

Fuente: elaboración propia.

4.2.3. Gestión/monitoreo

Un punto muy importante a tener en consideración a la hora de implementar cualquier proyecto de redes es la gestión y el monitoreo posterior que sirve para un mejor manejo operativo al momento de habilitar o deshabilitar servicios como a la hora de presentarse fallas en la red.

El monitoreo nos brinda la visión completa de una red sin poder intervenir en ella. La naturaleza del monitoreo es no intrusiva, el objetivo principal de la misma es el de darle una visión completa de lo que sucede en la red al operario de la misma así como alertar e indicar oportunamente cualquier falla que suceda en la misma.

La gestión de una red le brinda al operador de la red la intervención con todos sus elementos activos. Gracias a las bondades que presenta el protocolo TCP/IP se hace fácil hacer que la gestión sea no solo remota sino centralizada.

El monitoreo y la gestión de red son dos elementos que normalmente deben ir juntos para que los operarios de la red puedan contar con una herramienta 100 por ciento efectiva.

Al momento de implementar túneles IPv6, ya sean estos configurados o automáticos, se deberá validar los siguientes aspectos con el respectivo proveedor de equipos:

- Si se requiere de un *upgrade* de supervisoras en los equipos que establecerán los túneles, ¿estos podrán ser monitoreados y gestionados por el sistema de gestión y monitoreo actual?

- Si se requieren adquirir nuevas tarjetas de línea que soporten IPv6 en los equipos que establecerán los túneles, ¿estos podrán ser monitoreados y gestionados por el sistema de gestión y monitoreo actual?

- ¿El sistema de monitoreo y gestión actual será capaz de visualizar los túneles IPv6 a implementar?, ¿se requiere de licencias adicionales?

- ¿El sistema de monitoreo y gestión actual será capaz de dar de alta/baja y/o cambios a los túneles IPv6?, ¿se requiere de licencias adicionales?

- En caso de requerirse actualización del sistema de gestión, ¿la infraestructura actual donde se tiene instalado el sistema de monitoreo y gestión es capaz de soportar la nueva versión o se debe adquirir hardware adicional?

Si no se hace la revisión correcta de los puntos antes mencionados, al momento de ir ejecutando los pasos necesarios para implementar los túneles, existe el riesgo de ir perdiendo visibilidad y control sobre la red.

4.3. Ventajas y desventajas dentro de un ISP

Como todo protocolo, el ISP presenta diversas ventajas y desventajas que hacen viable o no su aplicación, esto dependiendo del fin que el mismo tendrá; de esta forma se presentan a forma de resumen sus principales características.

4.3.1. Coexistencia con una red IPv4 en producción

La técnica de transición de túneles manuales y automáticos es una técnica que permite una coexistencia y compatibilidad adecuada en una red IPv4 lo cual le brinda al administrador de red la flexibilidad y tranquilidad de iniciar a dar servicios IPv6 sobre una red IPv4 sin afectar los servicios actuales IPv4 que ya brinda por medio de esta red.

4.3.2. Afectación de servicios actuales

Este punto se divide en dos: una red IPv4 que ya soporta IPv6 y una red IPv4 que ya sea parcial o totalmente no soporta IPv6.

Para el primer escenario, la afectación de servicios es nula. El segundo escenario si presenta afectación de servicio. Esto, lógicamente es una limitante que se presentará con cualquier técnica de transición.

4.3.3. Alta disponibilidad

Se ha demostrado que la técnica permite el uso de protocolos de redundancia L2 y L3 adicionales al mecanismo de túneles *back-up* que brindan los túneles. Es importante hacer ver al lector que los túneles manuales no manejan ese mecanismo de manera automática como lo hacen los túneles automáticos y que los tiempos de convergencia ahí dependen de los tiempos que le conlleve al operador de red re-establecer los túneles.

4.3.4. Habilitación servicios E2E

Esta técnica permite la habilitación de servicios IPv6 E2E de manera parcial en la red y bajo demanda. En otras palabras, esta técnica permite focalizar esfuerzos en las partes de la red donde se hace necesario iniciar a dar los servicios sin tener que intervenir en otros puntos de red.

4.3.5. Habilitación de servicios internet

Esta característica permite al administrador de red focalizar los esfuerzos en los equipos de borde (*edge*) y en las partes de la red donde se desea iniciar a brindar el servicio.

4.3.6. Diseño y control

El implementar túneles es un tema que a nivel de diseño y control no es tan sencillo. Se debe tener un buen diseño para que la técnica sea escalable. Un mal diseño conlleva a una escalabilidad pobre. De igual manera, aun contando con un buen diseño, el tema de control vuelve más compleja la red, complicando lógicamente el control de la misma.

4.3.7. Fallas en la red

Al momento de presentarse fallas en la red y en específico en los servicios IPv6 que se estén brindando por medio de túneles manuales y/o automáticos el poder detectar las fallas es más complejo. Se debe contar con personal con un nivel de expertise alto (personal N2 o superior) para poder garantizar la disponibilidad de la red.

4.3.8. Escalabilidad

Esta técnica brinda una alta escalabilidad, sin embargo, el lector debe tener en cuenta que la alta escalabilidad irá de la mano de un buen diseño. Un mal diseño limitará sustancialmente la escalabilidad de la solución.

Tabla XV. **Ventajas y desventajas de implementar túneles IPv4 – IPv6**

Aspecto	Ventaja	Desventaja
Coexistencia con una red IPv4 en producción	✓	
Afectación de servicios actuales		
Si la red actual ya soporta IPv6	✓	
Si la red actual total no soporta IPv6 total o parcialmente		✓
Alta disponibilidad	✓	
Habilitación del servicio E2E	✓	
Habilitación del servicios Internet	✓	
Diseño y control		✓
Troubleshooting		✓
Escalabilidad	✓	

Fuente: elaboración propia.

CONCLUSIONES

1. Las redes de datos de los proveedores de servicio deberán, eventualmente, ser migradas de IPv4 a IPv6 por la escases de direcciones IPv4 a nivel mundial.

2. El protocolo actual IPv4 como el futuro IPv6 se encargan de definir los mecanismos de direccionamiento y enrutamiento manual o automático dentro de las redes de datos de los proveedores de servicio.

3. Cada una de las tres técnicas de transición expuestas en este trabajo de graduación (túneles IPv4 – Ipv6, doble pila y traductores IPv4 – Ipv6) presentan ventajas y desventajas, que se propone considerar al momento de ser implementadas como técnicas de transición de IPv4 a IPv6 en las redes de datos de los proveedores de servicio.

4. Los túneles, como técnica de transición de IPv4 a IPv6 en redes de datos de proveedores de servicio, permitirán la coexistencia entre las dos redes (IPv4 e IPv6) brindando una transición escalable y de alta disponibilidad sin afectar los servicios IPv4 actuales.

RECOMENDACIONES

1. Analizar y considerar las distintas ventajas y desventajas que cada una de las técnicas de transición de IPv4 a IPv6 presentan al momento de la planificación de transición de IPv4 a IPv6 en redes de datos de proveedores de servicio.

2. Considerar temas como alta disponibilidad, escalabilidad y control; así como la seguridad y movilidad de la red y cuantificar el impacto en la red IPv4 actual en producción al momento de implementar los túneles (manuales y/o automáticos) en redes de datos de proveedores de servicio.

BIBLIOGRAFÍA

1. AHUATZIN SÁNCHEZ, Gerardo L. *Desarrollo de un esquema de traducción de direcciones* IPv6-IPv4-IPv6. España, 2008. 94 p.

2. HAGEN, Silvia. IPv6 *Essentials*. Estados Unidos, 2011. 114 p.

3. JORDAN, Steve. CCDA 3RD Edition. Estados Unidos: Cisco Press, 2007. 688 p.

4. ODOM, Wendell. *CCENT/CCNA ICND1*. Estados Unidos: Cisco Press, 2008. 685 p.

5. ORTEGA, Xavier. *Radiaciones Ionizantes*. España: Universidad Politécnica de Catalunya, 1994.

6. SPALTER, Michael. Real *World* IPv6. Estados Unidos, 2012. 61 p.