UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL

FACULTAD DE CIENCIAS DE LA INGENIERÍA E INDUSTRIAS

CARRERA DE INGENIERÍA INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

Conectividad remota cliente - servidor a través de túneles IPv6 y seguridad IPSec, en ambientes multiplataforma.

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO

DE INGENIERO EN INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

CRISTIAN OSWALDO POZO NAZATE

DIRECTOR: ING. BOLIVAR JACOME

Quito, Marzo 2017

© Universidad Tecnológica Equinoccial. 2017
Reservados todos los derechos de reproducción

UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL

BIBLIOTECA UNIVERSITARIA

FORMULARIO DE REGISTRO BIBLIOGRÁFICO

PROYECTO DE TITULACIÓN

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	040150394-1
APELLIDO Y NOMBRES:	POZO NAZATE CRISTIAN OSWALDO
DIRECCIÓN:	DÍAZ DE LA MADRID Y JUAN ACEVEDO BALCON METROPOLITANO
EMAIL:	Cros_p11@yahoo.com
TELÉFONO FIJO:	
TELÉFONO MOVIL:	0980393225

DATOS DE LA OBRA	
TITULO:	CONECTIVIDAD REMOTA CLIENTE SERVIDOR A TRAVES DE TÚNELES IPv6 Y SEGURIDAD IPSEC EN AMBIENTES MULTIPLATAFORMA.
AUTOR O AUTORES:	CRISTIAN POZO
FECHA DE ENTREGA DEL PROYECTO DE TITULACIÓN:	**23 DE MARZO DE 2017**
DIRECTOR DEL PROYECTO DE TITULACIÓN:	ING. BOLIVAR JÁCOME
PROGRAMA	**PREGRADO** [x] **POSGRADO** [ ]
TITULO POR EL QUE OPTA:	INGENIERO EN INFORMATICA Y CIENCIAS DE LA COMPUTACIÓN
RESUMEN:	Esta investigación hace un estudio y análisis de la conectividad remota cliente servidor en la transición y coexistencia de redes IPv4 e IPv6 a través de túneles IPV6 y seguridad IPsec, utilizando herramientas de software libre, en ambientes virtualizados. Con un diseño de red que se basó en la metodología PPDIOO de Cisco, y un esquema de direccionamiento

	LAN-WAN con direcciones públicas IPV4 para las conexiones WAN y unicast global IPv6 para las redes LAN. Para el análisis de túneles y seguridad se utilizó herramientas de mapeo de puertos, análisis de tráfico y escaneo de acceso a equipos.
PALABRAS CLAVES:	Túneles, doble pila, 6to4, ISATAP, ISP, VPN, IPsec.
ABSTRACT:	This investigation makes a study and analysis of remote client server connectivity in the transition and coexistence of IPv4-only and IPv6-only networks through IPV6 tunnels and IPsec security using open source tools in virtualized environments. With a network design that was based on the Cisco PPDIOO methodology, and a LAN-WAN addressing scheme with public IPV4 addresses for WAN connections and global IPv6 unicast for LAN networks. For the analysis of tunnels and security we used port mapping tools, traffic analysis and equipment access scanning.
KEYWORDS	Tunnels, dual-stack, 6to4, ISATAP, TEREDO, ISP, VPN, IPsec.

Se autoriza la publicación de este Proyecto de Titulación en el Repositorio Digital de la Institución.

f:_____

CRISTIAN OSWALDO POZO NAZATE

040150394-1

UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL

BIBLIOTECA UNIVERSITARIA

DECLARACIÓN Y AUTORIZACIÓN

Yo, **POZO NAZATE CRISTIAN OSWALDO,** CI: 040150394-1 autor del proyecto titulado: **CONECTIVIDAD REMOTA CLIENTE SERVIDOR A TRAVÉS DE TÚNELES IPv6 Y SEGURIDAD IPsec, EN AMBIENTES MULTIPLATAFORMA** previo a la obtención del título de **INGENIERO EN INFORMATICA Y CIENCIAS DE LA COMPUTACIÓN** en la Universidad Tecnológica Equinoccial.

1. Declaro tener pleno conocimiento de la obligación que tienen las Instituciones de Educación Superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la BIBLIOTECA de la Universidad Tecnológica Equinoccial a tener una copia del referido trabajo de graduación con el propósito de generar un Repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Quito,23 de Marzo del 2017

f:_____

POZO NAZATE CRISTIAN OSWALDO

040150394-1

DECLARACIÓN

Yo **POZO NAZATE CRISTIAN OSWALDO**, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

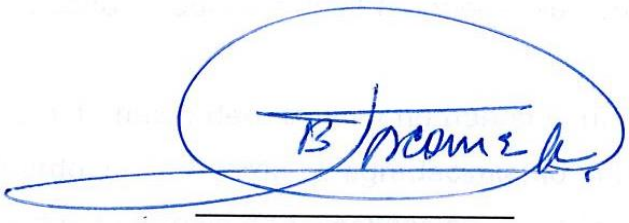
La Universidad Tecnológica Equinoccial puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

POZO NAZATE CRISTIAN OSWALDO

040150394-1

CERTIFICACIÓN

Certifico que el presente trabajo que lleva por título **Conectividad remota cliente - servidor a través de túneles IPv6 y seguridad IPsec, en ambientes multiplataforma**, que, para aspirar al título de **Ingeniero en Informática y Ciencias de la Computación** fue desarrollado por **Cristian Pozo**, bajo mi dirección y supervisión, en la Facultad de Ciencias de la Ingeniería e Industrias; y cumple con las condiciones requeridas por el reglamento de Trabajos de Titulación artículos 19, 27 y 28.



Ing. Bolívar Jácome

DIRECTOR DEL TRABAJO

C.I. 170700461-8

DEDICATORIA

El presente trabajo va dedicado a Dios por darme vida, salud, a la vez permitirme tener y disfrutar a mi familia, a mis padres que son el pilar fundamental, gracias a su esfuerzo, sacrificio, apoyo incondicional, por el interés mostrado para que estudie, y me desarrolle completamente en todos los aspectos de mi vida, son mi principal motivación para seguir adelante y por ellos logré culminar mi carrera.

De igual forma a mi hermana por ayudarme a crecer y madurar junto con ella, por estar junto a mí tanto en los buenos como en los malos momentos brindándome siempre todo su apoyo y consejos oportunos; a mi familia en general por nunca dejarme de lado a pesar de la distancia siempre están pendientes de mí recordándome que puedo contar con cada uno de ellos; A mis amigos, docentes y todas las personas que de una u otra forma me ayudaron, son muchos a quienes debo reconocer su contribución.

Algunos tal vez ni lo recuerden, incluso no han sido muy conscientes de su aporte, les guardo un recuerdo y agradecimiento muy particular por su colaboración con este trabajo de investigación. A todos ustedes gracias por todo.

ÍNDICE DE CONTENIDOS

PÁGINA

ÍNDICE DE TABLAS

PÁGINA

ÍNDICE DE FIGURAS

PÁGINA

RESÚMEN

Esta investigación hace un estudio y análisis de la conectividad remota cliente servidor en la transición y coexistencia de redes solamente IPv4 y solamente IPv6 a través de túneles IPV6 y seguridad IPsec, utilizando herramientas de software libre, en ambientes virtualizados. Con un diseño de red que se basó en la metodología PPDIOO de Cisco, y un esquema de direccionamiento LAN-WAN con direcciones públicas IPV4 para las conexiones WAN y unicast global IPv6 para las redes LAN. Para el análisis de túneles y seguridad se utilizó herramientas de mapeo de puertos, análisis de tráfico y escaneo de acceso a equipos.

Palabras clave: Túneles, doble pila, 6to4, ISATAP, ISP, VPN, IPsec.

ABSTRACT

This investigation makes a study and analysis of remote client-server connectivity in the transition and coexistence of IPv4-only and IPv6-only networks through IPv6 tunnels and IPsec security, using open source tools in virtualized environments. Whit a network design that was based on the Cisco PPDIOO methodology, and a LAN-WAN addressing scheme whit connection WAN IPv4 address and LAN networks global IPv6 unicast addressing. For the analysis of tunnels and security we used port mapping tools, traffic analysis and equipment access scanning.

Keywords: Tunnels, dual-stack, 6to4, ISATAP, ISP, VPN, IPsec.

1. INTRODUCCIÓN

Según la revista Computerworld en su edición "*Data Driven Businness*" menciona con la aparición del internet de las cosas[1], hace imprescindible proporcionar direcciones IP[2] a más dispositivos, estimando para el año 2020 habrá más de 50 mil millones de cosas conectadas a internet. La versión actual que predomina en internet es la versión 4 que con una longitud de 32 bits impide el crecimiento de la red, siendo el principal motivo que impulsó al desarrollo de una nueva versión que es la IP versión 6 o IPv6 llamado IP de la siguiente generación, pero antes se desarrolló el protocolo experimental versión 5 denominado ST-II[3] que nunca llego a utilizarse en la práctica.

Se estima que IPv6 no va a ser implementado completamente ni en corto ni mediano plazo, debido a que internet se ha convertido en algo vital en el mundo con IPv4 como el protocolo predominante. Al no ser compatibles las dos versiones del protocolo IP la migración requiere de una infraestructura que soporte dispositivos con esta nueva versión, por tal motivo no es posible su sustitución inmediata. (Dave Evans, 2011)

Para seguir utilizando IPv4 y retrasar la necesidad tanto del cambio como de los costos que esto implica, IETF[4] diseñó una serie de mecanismos de transición y coexistencia entre estos protocolos para lograr una migración transparente para el usuario final y progresiva a nivel mundial; la presente investigación se enfoca en la conectividad a través de la utilización de túneles y con las garantías que se exige actualmente de autenticidad, confidencialidad y confiabilidad para los datos que se trasmiten, también se aborda un mecanismo de seguridad que se llama IPsec.

[1] Internet de las cosas. - Interconexión de dispositivos electrónicos a internet.
[2] Dirección IP. – Número único con el que se identifica un dispositivo en la red.
[3] ST-II. – (Stream Protocol versión 2) Protocolo de transmisión de voz, video y simulación distribuida.
[4] IETF. – En español, Grupo de trabajo de ingeniería de internet.

Este trabajo de titulación tiene como objetivo desarrollar una conectividad remota cliente – servidor para las PIMES[5] que cuentan con un una matriz y sucursales en diferentes ciudades a través de túneles IPv6 y seguridad IPsec en ambientes de servidores multiplataforma. Para lo cual es necesario primeramente hacer una descripción de las características y funcionamiento de los túneles IPv6, sus tipos de configuración, transmisión de tráfico, seguidamente se debe seleccionar la metodología más adecuada para el desarrollo del proyecto y finalmente realizar el análisis de los resultados en función de cada una de las fases de la metodología seleccionada.

[5] PIMES. – Pequeña y mediana empresa.

2. MARCO TEÓRICO

En este apartado se habla de tres puntos principales que sirven para sustentar el presente trabajo: (1) Descripción y características del protocolo de internet, en sus dos versiones (IPv4 e IPv6); (2) Se enumera los mecanismos de transición que se pueden aplicar durante el periodo de cambio y actualización, profundizando en el mecanismo de transición por medio de túneles, indicando las características, funcionamiento, tipos de configuración y transmisión de tráfico; y (3) Descripción, características y funcionamiento de seguridad IPsec; (4) Descripción de metodologías de diseño de redes.

2.1. PROTOCOLO IPV4

Es el protocolo más utilizado e implementado en la interconexión de redes a gran escala y se encuentra en la capa de red, como parte del conjunto de protocolos de TCP/IP. Su función principal es asignar una serie de números decimales separados por puntos, que representara una dirección única; se utiliza de identificación de un dispositivo en internet para poder enviar y recibir datos con otros dispositivos. IPv4 se diseñó como un protocolo de bajo costo por lo que no verifica ni administra el flujo de paquetes, estas funciones las realizan las capas superiores, simplemente provee las funciones necesarias para procesar los datos de direccionamiento enviando cada paquete desde el origen a su destino. (Fierro & Arrieta, 2015)
Como principales características de IPv4 tenemos:

- ✓ **Direcciones de 32 bits. -** Brinda un máximo de 4.294.967.296 millones de direcciones únicas, distribuidas en 4 octetos de números de 0 a 255 separados por puntos. Se distribuyen por clases y existe

un gran número de direcciones reservadas para propósitos especiales como redes privadas.

- ✓ **Independiente de los medios físicos. -** Un paquete puede ser enviado por cualquier medio: guiado o no guiado
- ✓ **Protocolo no orientado a la conexión. -** No establece conexión previa entre el emisor y receptor antes de enviar el paquete, necesita campos adicionales en el encabezado de la PDU (protocolo de unidad de datos), con lo cual brinda un servicio de transferencia de paquetes no confiable
- ✓ **Mejor esfuerzo. -** No brinda ninguna garantía sobre el tráfico, su objetivo es generar la menor sobrecarga en la red, para la entrega de paquetes en menor tiempo

2.2. PROTOCOLO IPv6.

IETF lanzó en los años noventa el proyecto denominado Protocolo de Internet de Próxima Generación (IPng, por sus siglas en inglés) debido a los problemas y limitaciones que presenta IPv4. La Figura 1, muestra las principales diferencias entre las cabeceras. Los campos se encuentran con colores distintivos (Azul, Amarillo, Gris y verde) indicando lo siguiente azul indica los campos que se cambiaron de nombre, el color amarillo los campos que se mantienen, los campos de color gris indica los campos que se eliminaron y el campo de color verde es el campo que se agregó en el nuevo protocolo.

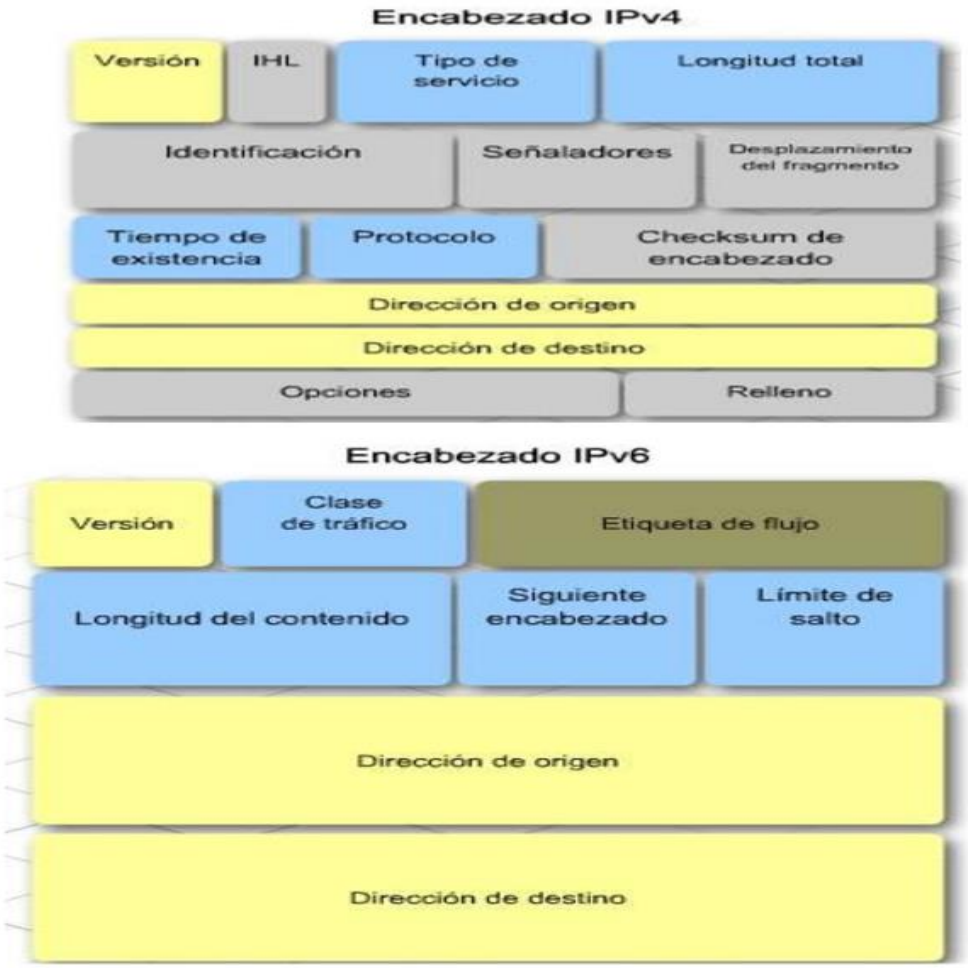


Figura 1. Diferencias entre las cabeceras IPv4 e IPv6. *(Cisco A. , 2015)*

La Tabla 1, se detalla las principales diferencias entre las dos versiones. En base a esto se puede destacar: IPv6 al poseer una cabecera fija obligatoria, mejora el rendimiento y velocidad de enrutamiento al momento del reenvío de paquetes. El tipo de servicio es reemplazado por la clase de servicio para identificar el tratamiento de tráfico.

Tabla 1. Principales diferencias entre IPv4 e IPv6

	Protocolo	
	Versión 4	**Versión 6**
Tamaño de direcciones	32 bits	128 bits
Tamaño cabecera	20 bytes	40 bytes
Formato de direcciones.	Notación decimal	Notación hexadecimal
Fragmentación	Lo realizan los routers y equipos	Lo realizan solo los equipos
Resolución de direcciones	Broadcast ARP	Vecino cercano
IPsec	Opcional	Obligatorio

2.2.1. DIRECCIONAMIENTO IPv6

Según el manual "*Preparing an IPv6 address Plan*" las direcciones ipv6 presentan una longitud de 128 bits para interfaces y conjuntos de interfaces, dividido en 8 grupos de 16 bits, separados por ":", representados por dígitos hexadecimales entre los que está permitido utilizar: caracteres mayúsculas o minúsculas, omitir ceros a la izquierda y representar una sola vez ceros continuos mediante "::". La Figura 2, muestra la estructura básica de una dirección IPv6 dividida en 3 partes para formar su esquema de direccionamiento.

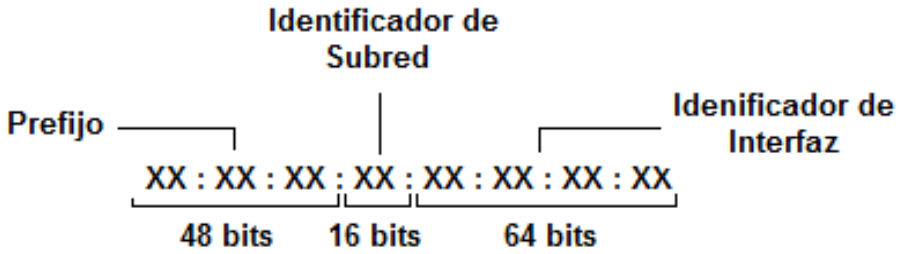


Figura 2. Estructura básica de una dirección IPv6. *(Oracle, 2012)*

La asignación de direcciones se lo hace a interfaces individuales en los nodos. La Tabla 2, muestra una breve descripción de los tipos de encaminamiento que se encuentran en IPv6 y corresponden a identificadores para interfaces o grupo de interfaces.

Tabla 2. Tipos de direccionamiento IPv6. *(Beijnum, 2006)*

Tipo	Descripción	Sub-Tipo
Unicast	Conexión y entrega uno a uno.	- Enlace local - Unicast globales
Multicast	Capacidad de escalabilidad mejorada de conexión y entrega una interfaz a un conjunto de interfaces.	- Asignada - No solicitada
Anycast	Se envía un paquete de una interfaz al grupo Anycast a la interfaz más cercana.	- Agregable global - Sitio local - Enlace local

2.3. TRANSICIÓN IPV4 A IPV6

Actualmente se encuentran mecanismos definidos en los RFC[6] publicados por el grupo de trabajo denominado transición de la siguiente generación (NGTRASN, por sus siglas en inglés); grupo que fue creado por la IETF que ayuda al desarrollo, convivencia y transición progresiva entre IPv4 e IPv6. Entre los principales mecanismos tenemos: Doble Pila (dual stack), Túneles (Manual, 6 to 4, ISATAP) y Traducción (traffic translation). (Jamhour, Storoz, & Maziero, 2003)

2.3.1. DOBLE PILA

Como muestra la Figura 3, las dos versiones de protocolos IPv4 e IPv6 están presentes de manera simultánea en un nodo, con la capacidad de

[6] RFC. – Request for coment publicaciones de IETF que describen aspectos de funcionamiento de internet.

enviar y recibir paquetes directamente y se denominan nodos IPv4/IPv6, facilitando a los nodos y aplicaciones la flexibilidad para establecer sesiones extremo a extremo sobre IPv4 o IPv6; resulta la manera más sencilla de manejar e intercomunicarse entre las infraestructuras desplegadas en IPv4 o IPv6, y logrando una convivencia indefinida hasta que pueda completarse la migración. (Fierro & Arrieta, 2015)

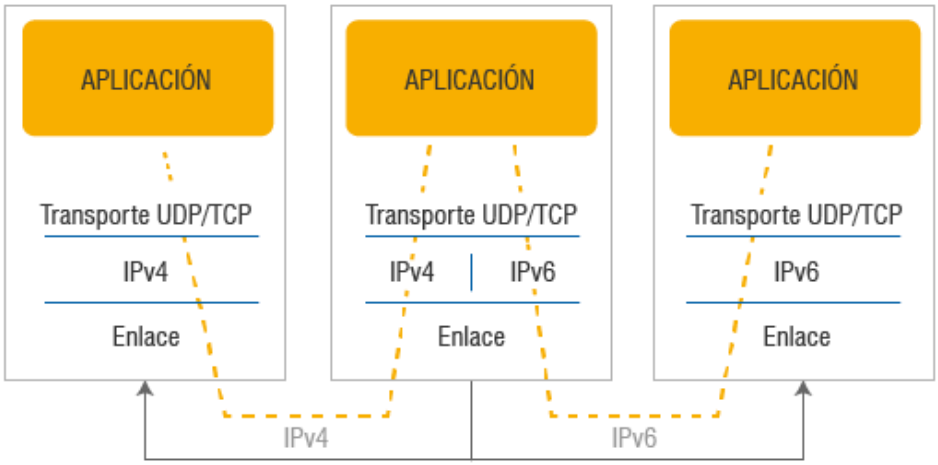


Figura 3. Diagrama general de doble pila

(Fuente: http://portalipv6.lacnic.net/dual-stack-o-pila-doble/)

2.3.2. TÚNELES

Proporcionan un enlace virtual extremo a extremo habilitando la conectividad los dos puntos. Su función incluye encapsulación, des-encapsulación y señalización de los extremos del túnel sin que se requiera la intervención de las capas superiores. La Figura 4, muestra La encapsulación de un protocolo en otro permitiendo transportar dicho paquete sobre una infraestructura por la cual el protocolo original no podría realizarlo. El extremo inicial del túnel es el encargado de hacer la encapsulación para poder realizar el transporte, al llegar a su destino o extremo final el encabezado del protocolo utilizado como transporte es eliminado para poder

des-encapsular y procesar el paquete como si hubiese sido enviado a través de una red nativa. (Cisco, 2007)

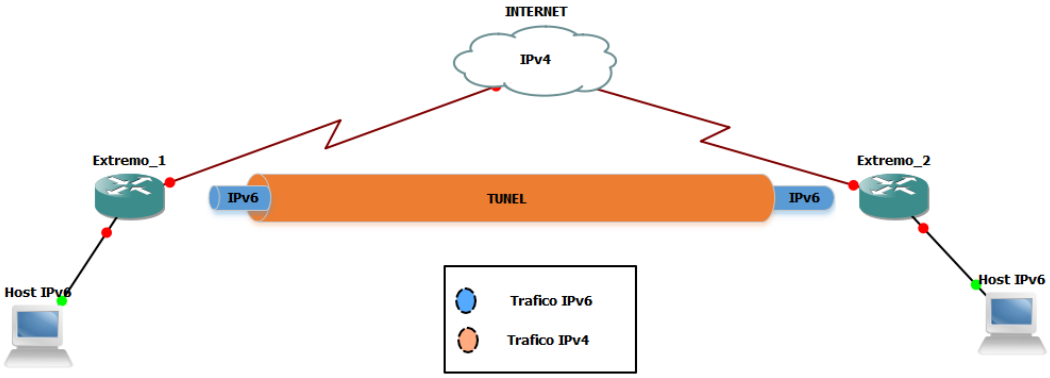


Figura 4.Diagrama básico de un túnel

2.3.3. TRADUCCIÓN

Utiliza dispositivos de red como NAT en IPv4 para poder comunicarse entre los protocolos IPv4 e IPv6 sin necesidad de requerir Dual Stack en los nodos pudiendo así convertir paquetes IPV6 en IPv4 y viceversa. Como principales ejemplos de traducción tenemos:

- SIIT (Stateless IP/ICMP Translation) que traduce la cabecera IP de IPv4 a IPv6 y viceversa.
- NAT-PT (NAT Protocol Translation) su forma de traducir es reemplazando la cabecera IPv6 con una IPv4.

Sin embargo, esta traducción viene con algunos inconvenientes lo que no permite solventarlos al coexistir los dos protocolos, uno de ellos es que se pierde la conexión punto a punto, por lo cual la red se encuentra vulnerable a ataques como spofin, DoS, entre otros, también para la traducción de direcciones es necesario una reescritura de la dirección y el puerto que se

encuentra conectado, y también recalcular el cheksum de TCP/UDP. (Fierro & Arrieta, 2015)

2.4. TÚNELES IPV6

Es un enlace bidireccional punto a punto entre los extremos de las redes que se van a comunicar, permitiendo una comunicación de forma estable y transparente entre nodos[7]; específicamente con direccionamiento IPv6 que se encuentran separados físicamente por una infraestructura IPv4, misma que se la utiliza como un enlace virtual. (Cisco, 2007)

La Figura 5, presenta el diagrama básico de un túnel y como se realiza la encapsulación en los extremos del túnel que vienen hacer los router de tipo doble pila. Son los encargados de administrar los paquetes que son transportados por la infraestructura IPv4.

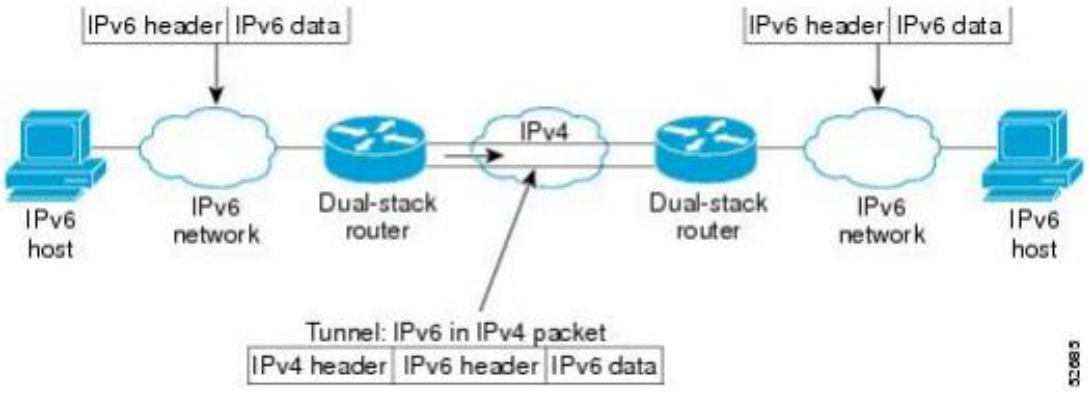


Figura 5: Diagrama general de Túnel IPv6. *(Cisco, 2012)*.

[7] Nodo. - Se denomina a un punto de intersección o unión de varios elementos (e. router) o conexiones a dispositivos finales (computador).

Según el caso de estudio realizado por la IJCSIS[8] en la universidad de Mysore en la India denominado "*IPv6 an IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model*"; Tenemos dos formas de crear túneles: de forma manual y automática. En los túneles manuales la comunicación entre extremos debe ser previamente establecida con la dirección de cada extremo final configurada de forma estática, normalmente se utilizan para túneles de punto a punto (entre router) con un identificador en el campo protocolo = 41.

La desventaja de la configuración manual se debe a una carga abrumadora a quienes administran la red en empresas corporativas globales que tienen que configurar cada túnel manualmente.

En los Túneles automáticos se determina automáticamente el extremo final al cual va dirigido el paquete, es decir, son conexiones punto – multipunto y emplean direcciones IPv6 basados en direcciones IPv4, en caso de la dirección IPv6 sea de tipo nativa, no se puede enviar un paquete mediante túnel automático. Actualmente se definen diferentes mecanismos que permiten la configuración de túneles:

Manual:

- ✓ 6 sobre 4
- ✓ GRE

Automático:

- ✓ ISATAP
- ✓ 6 to 4
- ✓ Teredo

Semiautomático:

- ✓ Túnel bróker

[8] IJCSIS. - Revista Internacional de Informática y Seguridad de la Información.

2.4.1. TÚNEL 6 SOBRE 4

Se considera un túnel tipo IP in IP, lo que significa que la dirección ipv6 tiene embebida la dirección IPv4 en el identificador de la interfaz. Es importante señalar que para poder realizar este tipo de túnel se requiere que los extremos soporten doble pila (Dual Stack) y la infraestructura IPv4 tenga su capacidad de multicast habilitada. La Figura 6, muestra la estructura básica una dirección IPv6 y como se encuentran conformadas las direcciones definidas para los extremos del túnel; con 2002 como el principal identificador del tipo de túnel establecido con dicha dirección.

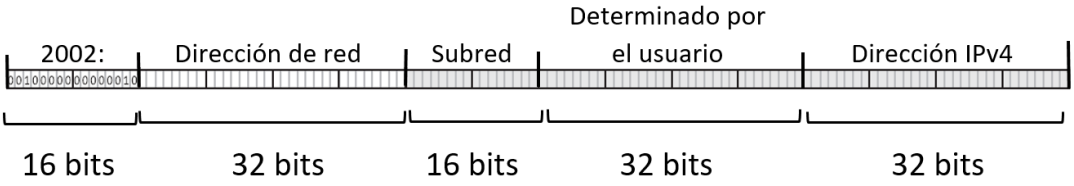


Figura 6: Formato de la dirección 6 sobre 4 *(IBM, 2016)*

2.4.2. TÚNELES DE ENCAPSULACIÓN DE ROUTING GENÉRICO

Encapsulación de enrutamiento genérico (GRE, por sus siglas en inglés), es un túnel manual, es decir, la configuración punto a punto se realiza de manera previa al envío de paquetes por medio del túnel; se considera como protocolo de tipo VPN sitio a sitio básico y no seguro por no poseer un mecanismo de seguridad sólido para proteger su contenido, pero con opciones para implementar seguridad. Fue desarrollado por Cisco y utilizado como túnel por defecto. En un router marca CISCO en caso de no especificar un protocolo, será el protocolo GRE el que se asigne a la conexión. (Cisco, 2016)

La Figura 7, muestra la encapsulación estándar de dos protocolos que realiza el túnel GRE, donde los campos pintados de color beige están los componentes del paquete original que va a ser transportado como un campo adicional en el paquete del protocolo nativo que se encuentra representado de color gris.

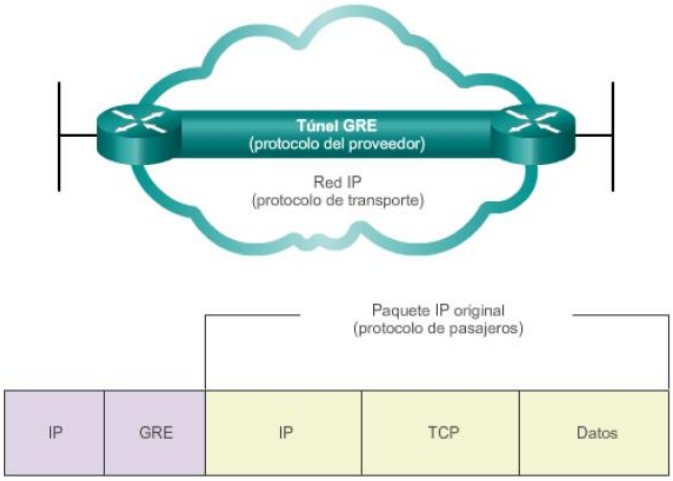


Figura 7. Encapsulación de paquetes con túnel GRE. *(Cisco A. , 2015)*

2.4.3. TÚNEL ISATAP

Por sus siglas en inglés, Intra Site Automatic tunnel addressing protocol; Su función es conectar entornos IPv6, que a pesar de encontrarse en un mismo entorno de red se encuentra separados por una red IPv4, es decir, permite crear túneles automáticos dentro de un sitio. (Beijnum, 2006)

A diferencia de 6 sobre 4, no necesita tener la función multicast habilitada y la infraestructura IPv4 se trata como una NBMA (no broadcast o difusion de acceso múltiple), la dirección IPv4 es codificada en la parte del identificador de interfaz de la dirección IPv6. La Figura 8, muestra el formato de la dirección IPv6 virtual, conformada con la concatenación del prefijo denominada dirección de enlace local que se trata de cualquier dirección

definida a partir de “FE80”. Como la dirección IPv4 ocupa la mitad del espacio de las direcciones disponibles locales, está precedida por dos secciones: el primero contiene un bit que indica si la dirección es globalmente única o Universal identificado por 0000: y única solo en la red local o local Bit identificado por 0200: y el bloque faltante siempre es “5EFE.

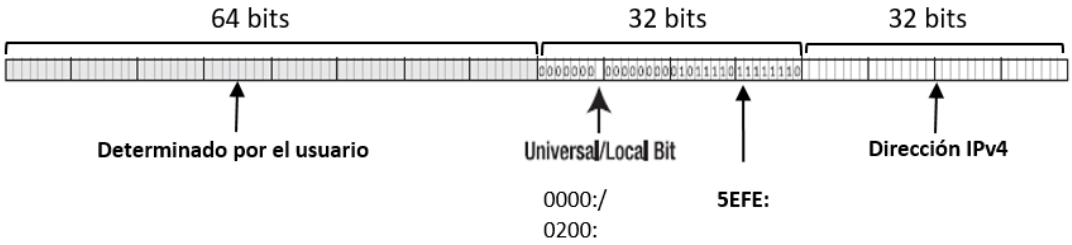


Figura 8: *Formato de la dirección ISATAP. (Beijnum, 2006)*

2.4.4. TÚNEL 6 to 4

Túneles automáticos punto a multipunto, al ser de este tipo solo puede tener enrutamiento estático. Su función es conectar redes IPv6 aisladas a través de una infraestructura IPv4 con direcciones públicas, permitiendo realizar un túnel entre sitios. La Figura 9, muestra la estructura de direccionamiento que se utiliza para realizar la conectividad por medio de túnel 6 to 4. Con su prefijo identificado por 2002: la dirección IPv4 que se va a concatenar a la dirección y la subred e identificador de red que se encuentran definidos por el usuario.

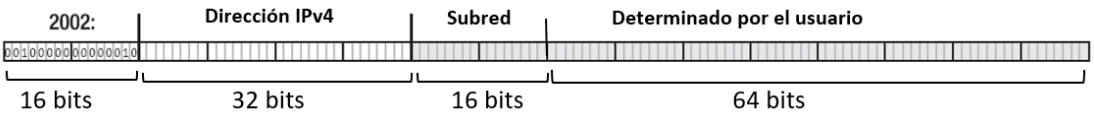


Figura 9: Formato de Direccionamiento de Túnel 6to4 *(Cisco, 2012)*

2.4.5. TEREDO

Es un túnel automático que funciona de manera similar a 6to4 con la diferencia que usa direcciones privadas, es decir garantiza la comunicación con islas IPv6 que se encuentras detrás un dispositivo NAT.

Opera con un protocolo de tunelización independiente de la plataforma que se está usando, está diseñado para proporcionar conectividad IPv6 por encapsulación de datagramas IPv6 dentro de un UDP IPv4. (Beijnum, 2006)

2.4.6. TÚNEL BRÓKER

Es una alternativa enfocada en la provisión de servidores dedicados llamado proveedores de túneles (tunnel brokers), usando un servicio basado en web para crear un túnel, donde el usuario se conecta para activar y registrar un túnel. El proveedor de túneles se puede ver como un ISP[9] virtual, registrando la dirección del usuario y el nombre en el DNS. Es escalable compartiendo la carga entre varios servidores de túnel (TS, por sus siglas en inglés).

Permite al ISP realizar fácilmente un control de acceso que se valida por medio de autentificación de usuarios, verificando su identidad; con lo que puede hacer cumplir las políticas establecidas para la utilización de recursos de la red. (Blanchet, Viangenie, & Parent, 2010)

[9] ISP. – Proveedor de servicio de internet.

2.5. SEGURIDAD IP

Conjunto de estándares que brinda confidencialidad, integridad y autenticación de los datos.

2.5.1. REDES PRIVADAS VIRTUALES

Es la conexión de una red privada a través de una red pública sin utilizar enlaces dedicados, con seguridad de encriptación y cifrado para garantizar la privacidad de los datos que se intercambian entre las redes privadas. (VPN en inglés Virtual Private Network), proporciona flexibilidad, escalabilidad, y menor costo. Su implementación se la puede realizar con un proveedor de servicio de internet local. (Cisco, 2013)

La Figura 10, presenta las características fundamentales con sus componentes que se deben implementar para tener una red virtual privada.

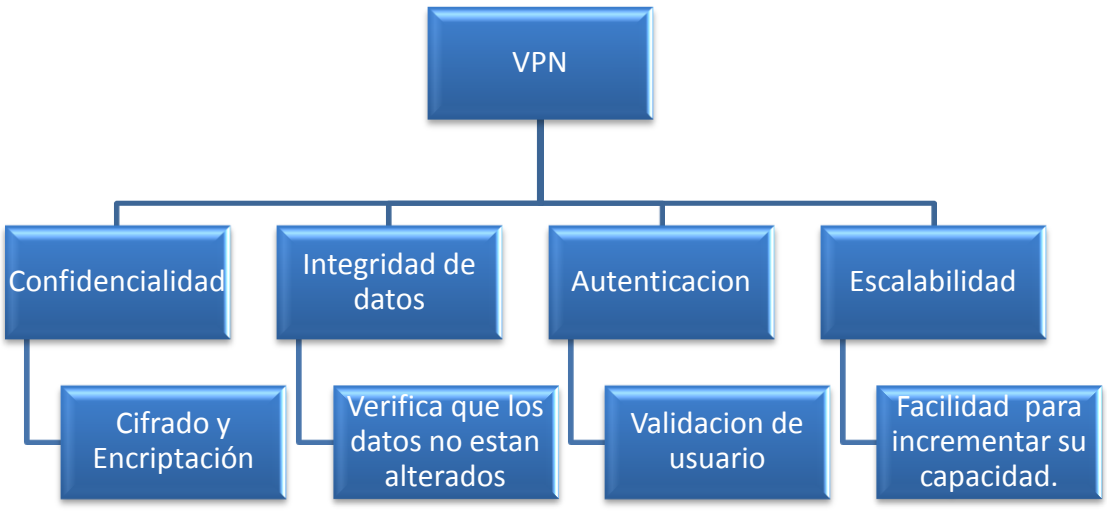


Figura 10. Características principales de VPN

2.5.2. PROTOCOLO DE SEGURIDAD IPsec

Es un conjunto de estándares independientes que se definen por etapas en un marco de trabajo para emplear servicios de seguridad a través de los cuales 2 dispositivos pueden establecer una comunicación de forma segura. La cabecera de IPsec se inserta a continuación de la cabecera IP y antes de los datos que se desea proteger, con lo cual se asegura la comunicación de extremo a extremo. (Franciscone, 2009)

La Tabla 3, describe los protocolos utilizados en IPsec y el tipo de seguridad de tráfico AH y ESP basándose en la distribución de claves criptográficas y el manejo de flujo por medio de la autenticación con control de acceso. Se los puede aplicar solos o combinados tanto para IPv4 como para IPv6. IPsec permite al administrador controlar el tipo de seguridad que se ofrece al paquete y las combinaciones que requiera la implementación en la comunicación.

***Tabla 3*.** Protección proporcionada AH y ESP en IPsec (Oracle,2014)

Protocolo	Protección de paquetes	Protección
AH **(**Cabecera de Autenticación**)**	Protege paquete del encabezado IP y de transporte, se define en el protocolo 51.	• Proporciona Integridad sólida, autenticación de datos. • Garantiza recepción de datos sin alteraciones. • Es susceptible a los ataques de repetición cuando AH no activa la repetición contra repeticiones(anti-repudio).
ESP **(**Carga de Seguridad Encapsulada**)**	Protege el paquete que sigue a ESP en el datagrama.	• Cifrado de datagrama IP. Garantiza la confidencialidad. • Autenticación. Proporciona la misma protección que AH. • Proporciona integridad sólida, autenticación de datos y confidencialidad.

2.5.2.1. Asociación de seguridad (SA)

Son acuerdos que deben establecerse para tener una conexión segura, como confidencialidad en él envió de datos con el uso de claves, las mismas que se deben conocer entre los extremos antes de iniciar una comunicación, también se debe acordar el nivel de seguridad que se requiere y los algoritmos a utilizar. Cada SA se aplica solamente a un protocolo (AH o ESP), al ser una conexión simplex–unidireccional el flujo que requiera en ambos protocolos se gestiona uno o más SA para cada uno y brindar un servicio bidireccional.

En toda comunicación que se realiza con IPsec se debe establecer mínimo una SA antes de enviar los datos. La asociación de seguridad se identifica por: un índice de parámetros de seguridad (SIP), la dirección IP de destino y el identificador de protocolo de seguridad (AH o ESP). (Franciscone, 2009)

2.5.2.2. Modo de operación

Los protocolos de seguridad AH y ESP soportan dos modos de uso que pueden ser:

- **Transporte. –** Se tiene confidencialidad protegiendo los datos en una comunicación entre host. En ESP proporciona seguridad a capas superiores, es decir, se excluye a cabecera IP y cualquier cabecera de extensión precedente de la cabecera ESP; y en AH se extiende la seguridad a las partes seleccionadas de la cabecera IP, cabecera de extensión y opciones seleccionadas.
- **Túnel. -** Protege el paquete IP completo, encapsulándolo dentro de otro. En esencia una SA aplicada a túnel IP, obligatorio cuando uno o ambos extremos se comportan como security Gateway (router o

firewall). Evita problemas en la fragmentación y re-ensamblado de paquetes, al igual que en circunstancias donde exista varios caminos por los cuales son transportados los paquetes IP. En AH aplica protección a todo el paquete IP al cual se hizo el túnel incluido las otras partes de la cabecera IP y en ESP se protege únicamente al paquete al cual se hizo el túnel o paquete tunelizado.

La Tabla 4, lista los principales parámetros que se pueden utilizar en la configuración con seguridad IPsec y las variantes que se pueden aplicar en cada uno de ellos dependiendo del nivel de seguridad que se quiera implementar.

Tabla 4. Parámetros para configuración de IPsec *(Oracle, 2012)*

Parámetro	Tipo
Algoritmo de hash o resumen	MD5
	SHA-1
Algoritmo de encriptación	DES
	3DES
	AES
Llave	Pre-shared
	Firma RSA
Versión de Diffie-Hellman	1,2 o 5
Tiempo de vida del túnel	Se define en segundos

2.6. METODOLOGÍAS DE DISEÑO DE REDES

Es un conjunto de procedimientos flexibles utilizados para hacer el proyecto manejable dividiéndolo en módulos que puede ser más fácil de mantener y cambiar.

2.6.1. TOP-DOWN

Top-Down se utiliza para diseñar redes que comienza en las capas superiores del modelo OSI antes de seguir con las capas inferiores. Se concentra en aplicaciones, sesiones y transporte de datos antes de la selección de los routers, switches y medios que funcionen en las capas inferiores.

Según los sistemas Cisco, recomienda un acercamiento modular con un modelo jerárquico de tres capas que son: Núcleo, distribución y capas de acceso. Con un acercamiento estructurado se puede trabajar cada módulo por separado y concentrándose en los requerimientos, aplicaciones y estructura lógica antes de la selección de dispositivos físicos y productos que se implementan en el diseño. El ciclo de vida está conformado las siguientes fases:

Análisis de requerimientos que se realiza el análisis de las metas de negocio, ventajas, desventajas y tráfico de las redes existentes. Desarrollo de diseño lógico donde se diseña la topología de la red, selección de protocolos y estrategias de mantenimiento y seguridad. Desarrollo de diseño físico se emplea esta fase para la selección de tecnologías y dispositivos que se implementaran. y su última fase está conformada por: probar, optimizar y documentar el diseño con la cual se entrega la información detallada del proyecto. (Priscilla Oppenheimer, 2011)

2.6.2. PPDIOO

Es una metodología de Cisco que por sus siglas en inglés se define con las fases que conforman el ciclo de vida continuo que son: Preparar, Planear, Diseñar, implementar, Optimizar, Operar. Su función principal es reducir costos en la infraestructura de red con la definición de los requisitos para implementar una nueva tecnología y el ciclo de vida flexible con la opción de no pasar por todas las fases necesariamente en el orden establecido, permitiendo cambios en las fases que ya se aplicaron. (Priscilla Oppenheimer, 2011)

En la Planificación se identifican todos los requerimientos detallados que son identificadas, así también realizar el estudio del estado actual de la red. Con el diseño: Se diseña de acuerdo con los requisitos y el estado de red consultando con el usuario o propietario. Implementación: En esta fase se procede a la creación de acuerdo con los diseños establecidos. Operación: En esta fase se realiza la operación y monitorización de la red y como también la respectiva comprobación final del diseño. Optimización: Fase donde se realiza las detecciones y correcciones de los problemas.

2.6.3. MCCABE JAMES

La implementación de la rede se dan en fases y procesos necesarios para implementar una nueva red que a partir de esta pueden sufrir cambios sin dañar su estructura. Esta metodología se divide en las siguientes fases: análisis, diseño lógico y diseño físico.

Fase de análisis se establecen los requerimientos como mapas de aplicaciones especificando la ejecución de forma distribuida a nivel de

campus y a nivel de computadoras. Con su flujo de datos simples y compuestos donde se valida el origen/destino, la capacidad, retardo y confiabilidad de toda la red involucrada.

Fase de diseño lógico se establecen las metas del diseño con su respectiva valuación de tecnología con lo que involucra costos, rapidez y confiabilidad.

Fase de diseño físico se realiza el diseño físico de la red con la evaluación del diseño de cableado, ubicación de equipos, asignación de direcciones y desarrollo de una estrategia de enrutamiento. (McCabe, 1997)

3. METODOLOGÍA

Este capítulo especifica los métodos científicos empleados para obtener la información necesaria para la elaboración de esta tesis y la metodología utilizada en el desarrollo practico de la investigación.

3.1. MÉTODOS CIENTÍFICOS

En este proyecto se utilizó varios métodos de investigación con los cuales permiten sustentar la fundamentación teórica.

La Tabla 5. Describe los métodos utilizados en el desarrollo del Proyecto.

Tabla 5. Resumen de los métodos de investigación aplicados

Métodos de investigación		**Aplicación**	**Fase de la investigación**
Teóricos	Inductivo	- Identificación del problema	Introducción
	Deductivo	- Diseño de la aplicación	Metodología
	Analítico - Sintético	- Selección de las fuentes de la información y elaboración de contenidos sistematizados de cada tema	Marco teórico
Empíricos	Simulación	- En el modelamiento virtual de la red con el fin de comprobar su funcionamiento	Análisis de resultados
	Experimentación	- Implementación de la topología de la red para verificar su funcionamiento	

3.2. METODOLOGIA DE DISEÑO DEL PROYECTO

Luego de la revisión de algunas metodologías detalladas en el marco teórico de la presente investigación. La metodología que se seleccionó para el desarrollo en este proyecto fue PPDIOO de Cisco, por su enfoque en definir las actividades mínimas requeridas para optimizar el desempeño a través del ciclo de vida de la red y la capacidad de brindar la flexibilidad necesaria para poder ajustar cambios en cada una de las fases. La Figura 11. muestra las fases en las que se encuentra dividido el ciclo de vida de la metodología, orden opcional que es establecido como estándar para un correcto desarrollo del proyecto.

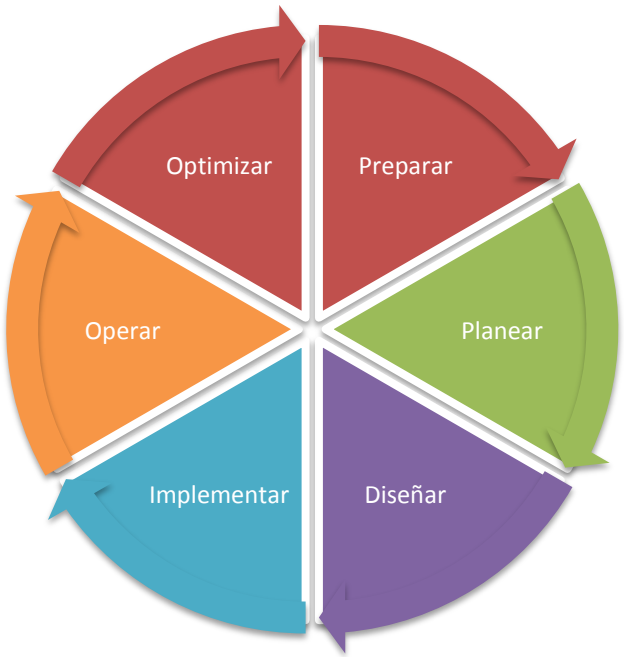


Figura 11. Fases de ciclo de vida PPDIOO

3.2.1. PREPARAR

En esta fase se realizó la recopilación de la información necesaria y requisitos para el desarrollo del proyecto. La información se encuentra documentada en el marco teórico y los requisitos se lo presenta en la entrega de resultados como también la definición de la línea base.

3.2.2. PLANEAR

De acuerdo a los requerimientos establecidos en la fase anterior se procede al detallar las especificaciones y características necesarias para la implementación del prototipo del proyecto. Se indica el diagrama funcional de la solución.

3.2.3. DISEÑAR

Elaboración de la topología de la red, el esquema de direccionamiento IPV6, los protocolos de enrutamiento, esquema lógico de la estructura y ubicación de los dispositivos como router, servidores y host.

3.2.4. IMPLEMENTAR

Se elaboró un cuadro comparativo de las diferentes características y costos de los dispositivos de la red a utilizar, lo cual facilitó seleccionar la mejor opción.

3.2.5. OPERAR

En esta fase se realizó las pruebas de conectividad y validación del funcionamiento entre los distintos puntos de la red.

3.2.6. OPTIMIZAR

Se hizo una comparación de los diferentes tipos de túneles para realizar ajustes de ser necesarios y así mejorar y optimizar el funcionamiento de la red.

4. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Se presentan los resultados obtenidos en cada etapa de la metodología de diseño de redes PPDIOO.

4.1.1. FASE PREPARAR

Para la implementación de túneles a nivel de una red corporativa, de acuerdo a la información recopilada y documentada en el marco teórico se puede definir los requerimientos para una correcta implementación del prototipo los cuales son: tener una infraestructura de una red LAN-WAN con un direccionamiento IPv6 en las redes LAN donde se encuentran distribuidas las sucursales y la matriz para un ambiente cliente servidor. Para la conexión de estas redes es necesario un direccionamiento IPv4 en los enlaces WAN.

Actualmente las empresas hacen uso de túneles GRE para la interconexión de usuarios remotos a la red corporativa, por lo tanto, se puede definir como la línea base para la presente investigación. (IPv6TF-EC, 2009)

4.1.2. PLANEAR

Para el desarrollo del proyecto, se estructuró una red LAN-WAN en un ambiente controlado en el laboratorio de la universidad UTE y el direccionamiento se asignó de la siguiente forma: direcciones unicast global en las redes LAN y direcciones publicas IPv4 para las redes WAN; todo esto en base a los requerimientos definidos en la fase anterior y para las

especificaciones del prototipo se tomó como ejemplo una empresa que tiene un modelo cliente/servidor con su oficina Matriz en Quito y una sucursal ubicada en la ciudad de Ibarra. Para la comunicación entre las dos oficinas se utilizó un enrutador que actuará como un ISP, cada oficina contará con un router con enrutamiento dinámico vector distancia y estado de enlace que serán los extremos del túnel.

4.1.3. DISEÑAR

La topología del prototipo utilizada es de tipo estrella (Ver Anexo1), con direcciones globales unicast IPv6 para redes LAN, direcciones públicas IPv4 para la red WAN y la dirección para cada túnel se estructuró de acuerdo a cada tipo (ver Anexo 2).

Para la conectividad de los enlaces WAN se realizó enrutamientos Estático, OSPF.

La Tabla 6. Muestra los sistemas operativos, y herramientas que se utilizaron para cumplir con el objetivo del presente trabajo.

Tabla 6. Sistemas operativos y herramientas utilizadas para la implementación de la red LAN- WAN IPV6/IPv4.

Sistema Operativo / Herramienta	Versión	Costo
Windows	7	135 $
CentOS	7	0.00 $
Oracle VM Virtual Box	5.1.14	0.00 $
Wireshark	2.2.4	0.00 $
GNS3	1.5.3	0.00 $
PUTTY	0.67	0.00 $
VPNClient	5.0.7.049	0.00 $

Al utilizar software libre en la mayoría de los sistemas operativos y herramientas necesarias para el desarrollo del prototipo del proyecto el costo de los aplicativos es de 135 $.

La Tabla 7. Muestra las características y costos unitarios de los materiales disponibles en el laboratorio de redes de la universidad UTE, con los cuales se realizó la conectividad del túnel y la seguridad implementada con IPsec.

Tabla 7. Recursos tecnológicos necesarios para recrear una red LAN-WAN IPV6/IPV4

Recurso	Marca	Modelo	Cantidad	Costo unitario
Router	Cisco	1800	3	586,00 $
Switch	Cisco	Catalyst 2960	2	758,00 $
Switch	Cisco	Catalyst 2950	1	700,00 $
Interfaz WAN	Cisco	WIC-2T	3	70,28 $
Cable serial DTE-DCE crossover	N/A	N/A	2	15,00 $
Adaptador serial	N/A	N/A	3	18,00 $
Cable de poder	N/A	N/A	5	4,00 $
Patch cord cat 5e	N/A	N/A	15	5,00 $
Laptop	Azus	A455L	1	800,00 $
Computador de laboratorio	Clones	N/A	4	500,00 $

Los costos para los materiales a utilizar fueron cotizados de las páginas de cisco, eBay y Amazon. Por lo tanto, el valor de la implementación puede variar dependiendo el proveedor. Para nuestro proyecto el valor total de los materiales utilizados es 7163, 84 $.

Para lo cual el costo total entre las herramientas, sistemas operativos y materiales que se utilizó. El costo total del prototipo es de 7298,84

4.1.4. IMPLEMENTAR

La Figura 12, muestra las conexiones de los equipos realizadas en el emulador GNS3, para luego realizar la respetiva configuración y análisis de conectividad de los diferentes tipos de túneles involucrados.

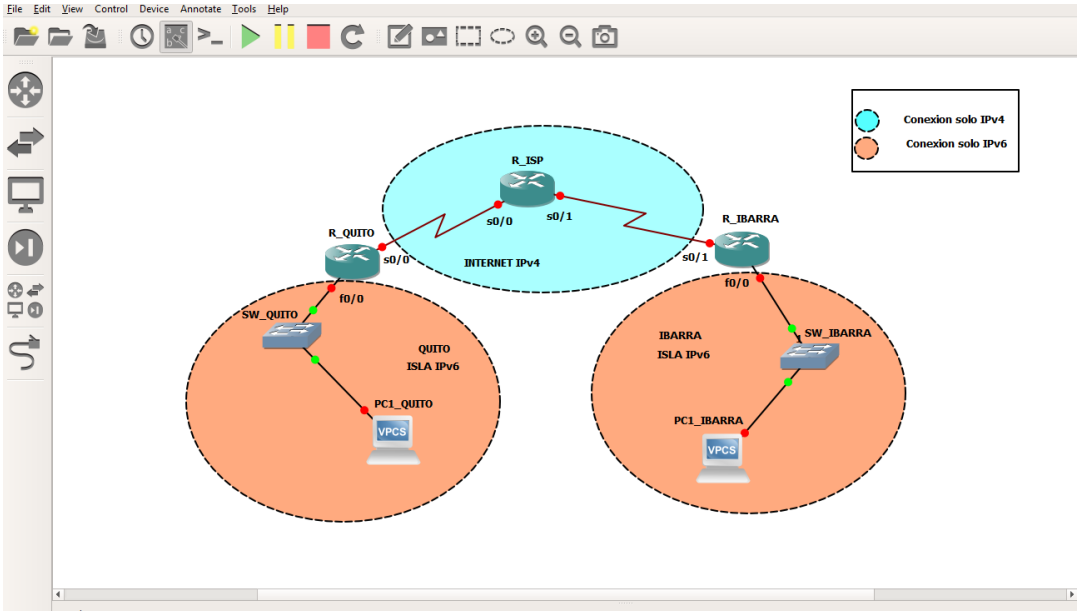


Figura 12.Conexion general de equipos en emulador GNS3 para análisis de túneles.

La Figura 13, muestra las conexiones físicas que se realizaron en los equipos utilizados para la implementación.

Figura 13. Conexión física de los equipos de networking del prototipo.

4.1.5. OPERAR

Aquí se realizaron las configuraciones y pruebas necesarias para tener una conectividad completa dentro de la red, junto con los túneles revisados en la presente investigación. Todas las configuraciones realizadas se basaron en el Anexo 2.

El detalle abajo escrito muestra la asignación de direcciones IPv6, IPv4 a Interfaces de los router de Ibarra, ISP y Quito,

Las configuraciones en el router Quito e ISP.

R_QUITO(config)#IPV6 unicast-routing→ se habilita enrutamiento unicast en IPv6.

R_QUITO(config)# interface fast ethernet 0/0→ ingreso a la interfaz FastEthernet0/0.

R_QUITO(config-if)#ipv6 enable→ habilitación de IPv6 en la interfaz.

R_QUITO(config-if)# ipv6 address 2001:db8:f0ca::1/64→se añade la dirección IPv6 a la interfaz.

R_QUITO(config-if)# no shutdown→se levanta la interface física.

R_QUITO(config)#int loopback 0→ Ingreso a la interfaz lógica loopback 0.

R_QUITO(config-if)#ip address 192.168.1.1 255.255.255.0→ Se asigna una dirección IP a la interfaz lógica.
R_QUITO(config-if)# no shutdown→se levanta la interface lógica.
R_ISP(config)# interface serial 0/0→ ingreso a la interface Serial.
R_ISP(config-if)# ip address 80.0.1.1 255.255.255.252→ asignación de dirección IPv4 y mascara de red.
R_ISP(config-if)# no shutdown→ se levanta la dirección en la interfaz.

EL proceso se lo realiza a todas las interfaces de los equipos que componen toda la red LAN-WAN.
Una vez realizada las asignaciones de las direcciones a cada dispositivo de la red se procedió a realizar el enrutamiento OSPFv3 en redes IPv6 y OSPF para redes IPv4.
A continuación, se muestra las configuraciones de enrutamiento realizadas en el router ISP para OSPF y en el router Quito el enrutamiento OSPFv3.

R_ISP(config)#> router OSPF 1→ Creación de direccionamiento ospf para direcciones IPv4.
R_ISP(config-router)#>network 192.168.1.0 0.0.0.255 area 0→ Ruta para loopback 0 del router R_QUITO.
R_ISP(config-ROUTER)#>network 80.0.1.0 0.0.0.3 area 0→ Ruta para enlace con R_QUITO.
R_ISP(config-ROUTER)#>network 80.0.2.0 0.0.0.3 area 0→ Ruta para enlace con R_IBARRA.
R_ISP(config-ROUTER)#>network 192.168.2.0 0.0.0.255 area 0→ Ruta para loopback 0 del router R_IBARRA.
R_QUITO(config)#> ipv6 router OSPF 1
R_QUITO(config-if)# router-id 1.1.1.1→ identificador de cada router por preferencia le ubique con 1.1.1.1 por referencia a r1 2.2.2.2 para r2... etc.
R_QUITO(config)#>interface Fast Ethernet 0/0

R_QUITO(config-if)#> ipv6 ospf 1 area 0→ se agrega la interfaz física para el enrutamiento ospf.

Se configura de igual manera los router de R_Quito, IPS y R_Ibarra tanto para OSPF y OSPFv3.

La Figura 14, muestra el archivo de configuración completo del router QUITO con un enrutamiento ospf para IPv4 y ospfv2 para las redes LAN IPv6 antes de realizar las pruebas con cada tipo de túnel.

```
R_QUITO#sh run
Building configuration...

*Mar  1 00:30:53.727: %SYS-5-CONFIG_I: C
Current configuration : 1634 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_QUITO
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:F0CA::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/0
 ip address 80.0.1.2 255.255.255.252
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/3
 no ip address
 shutdown
 clock rate 2000000
!
```

```
router ospf 1
 log-adjacency-changes
 network 80.0.1.0 0.0.0.3 area 0
 network 80.0.2.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Figura 14. Archivo de configuración router R_QUITO direccionamiento.

Una vez que se tiene asignadas las direcciones, el enrutamiento se encuentra correctamente configurado se procede a la configuración del túnel.

Para la sustentación de la presente investigación se realizaron diferentes tipos de túneles los cuales tienen una plantilla similar con algunas variaciones que a continuación se detallará el código de un extremo del túnel en el router R_Quito de cada tipo de túnel configurado.

R_QUITO(config) # interface tunnel 0
R_QUITO(config-if) #ipv6 address 2001:db8:f0ca:ac10:0c00::2/126 →dirección ipv6 asignada al extremo de túnel (debe ser única por lo que la mejor forma es embebida con la dirección ipv4) también se puede crear la dirección en base a la MAC address (EUI-64).
R_QUITO(config-if) #tunnel source loopback 0 → interfaz de la cual inicia el túnel (192.168.1.1/24)
R_QUITO(config-if) #tunnel destination 192.168.2.1→ Dirección del extremo final del túnel (solo aplica para la configuración de túneles estáticos IPv6IP y GRE).

Para la habilitación del modo del túnel, existe una opción para cada tipo de túnel; a continuación, se presenta los modos que se aplicaron a cada tipo de túnel.

R_QUITO(config-if) #tunnel mode ipv6ip→ Túnel manual, estático.

R_QUITO(config-if) #tunnel mode gre ip→ Túnel genérico de cisco.

R_QUITO(config-if) #tunnel mode ipv6ip 6to4→ Túnel automático 6to4.

R_QUITO(config-if) #tunnel mode ipv6ip isatap→ Túnel automático ISATAP.

Direcciones IPv6 de acuerdo al tipo de túnel que se emplea se utiliza un tipo de dirección.

La Figura 15, presenta la dirección que se genera con el asistente en el router utilizada para túnel automático 6to4 de acuerdo a la dirección IPv4 asignada a la interfaz serial.

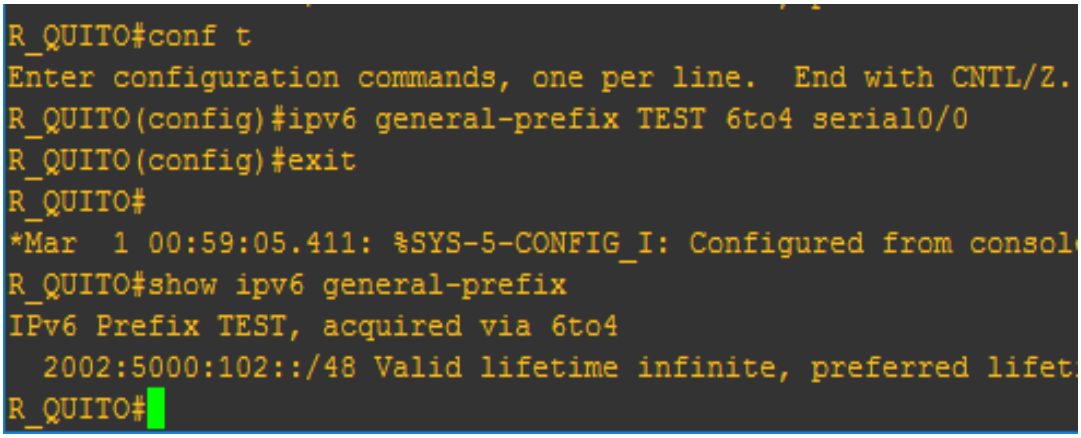


Figura 15. Resolución de dirección 6to4

La Figura 16, muestra la dirección asignada para el túnel ISATAP y la estructura de la dirección que se basó en la figura 8.

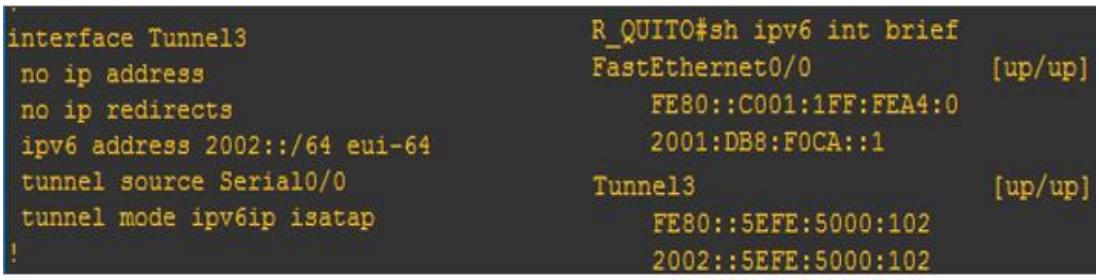


Figura 16. Asignación y estructura de dirección ISATAP

La Figura 17, muestra el archivo de la configuración de tres tipos de túneles GRE, IPV6IP, 6to4 en este caso se trata de túnel 0,1 y 2 respectivamente. Como el túnel GRE se genera de forma genérica no se muestra de forma explícita el tipo de túnel que se utiliza.

```
!
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8:B0CA::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source Serial0/0
 tunnel destination 172.16.13.2
!
interface Tunnel1
 no ip address
 ipv6 address 2001:AC1D:C00::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source Serial0/0
 tunnel destination 172.16.13.2
 tunnel mode ipv6ip
!
interface Tunnel2
 no ip address
 no ip redirects
 ipv6 address 2002:AC1D:C00::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source Serial0/0
 tunnel mode ipv6ip 6to4
!
```

Figura 17. *Archivo de configuración de túneles IPv6*

Una vez que se creó el túnel y se realizaron las pruebas de conectividad se procedió a la implementación de seguridad IPsec. A continuación, se muestra la configuración del router Quito con las fases de encriptación.

R_QUITO(config)# Crypto isackmp policy 10→

R_QUITO(config-isakmp)# encryption 3des→ tipo de algoritmo de encriptación

R_QUITO(config-isakmp)# Hash md5→ tipo de algoritmo de autenticación
R_QUITO(config-isakmp)# authentication pre-shared→ tipo de comunicación para el envío de la llave (KEY).
R_QUITO(config-isakmp)# group 2→ versión que se aplica de Diffie Hellman
R_QUITO(config-isakmp)# lifetime 3600→ asignación de tiempo al túnel IKE
R_QUITO(config)#crypto isakmp key 0 topsecret address 80.0.2.2→
R_QUITO(config)#Crypto ipsec transform-set set-60 esp-3des esp-md5-hamc→ negociación de parámetros de seguridad.

R_QUITO(config)# crypto ipsec profile ipsec-prof→ creación del perfil que se asignara la configuración de IPsec a una interfaz.
R_QUITO(ipsec-profile)# set transform set set-60→ asignación de transform-set al perfil.

R_QUITO(config)#int tunnel 0
R_QUITO(config-if)#tunnel protection ipsec profile ipsec-prof→ asignación del perfil IPsec a una interfaz

La Figura 18, muestra el archivo de configuración completo del router QUITO con el túnel GRE y la implementación de seguridad en el túnel.

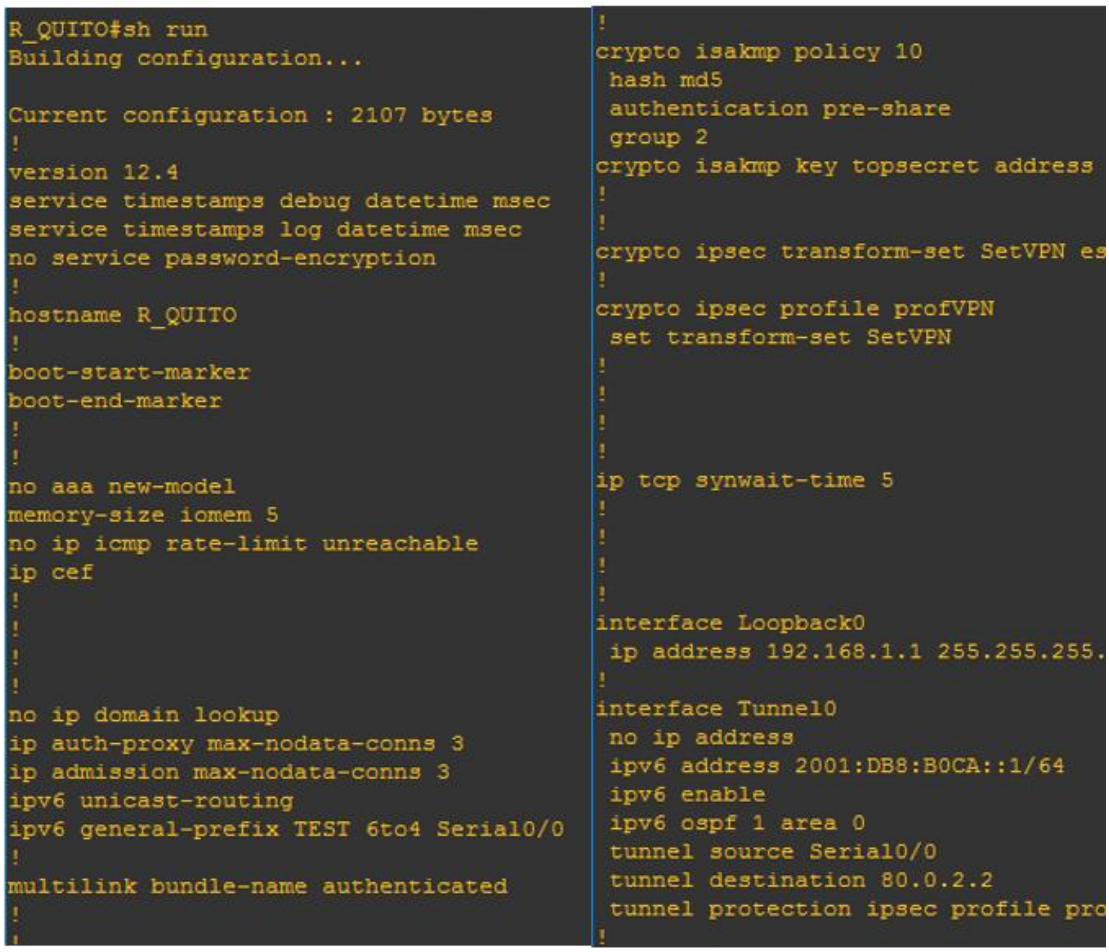


Figura 18. Archivo de configuración R_QUITO seguridad IPsec.

4.1.6. OPTIMIZAR

Se realizaron los distintos análisis de conectividad, enrutamiento y seguridad de los túneles y la elección del tipo de túnel que se ajusta más a la red aplicada para su implementación en los dispositivos físicos en el laboratorio de la universidad UTE.

A continuación, se muestran los resultados de análisis de cada tipo de túnel para transportar el tráfico IPv6 a través de una infraestructura IPv4.

La Figura 19, muestra la conectividad entre los extremos del túnel manual, para identificar cada punto se resaltó con un recuadro que indica: 1) la conectividad de las islas IPv6 y el tipo de tráfico que pasa a través del túnel manual en este caso ICMP, 2) especifica el número del protocolo que toma los paquetes IPv6 dentro del paquete IPv4, y 3) indica las direcciones físicas de origen y destino del túnel.

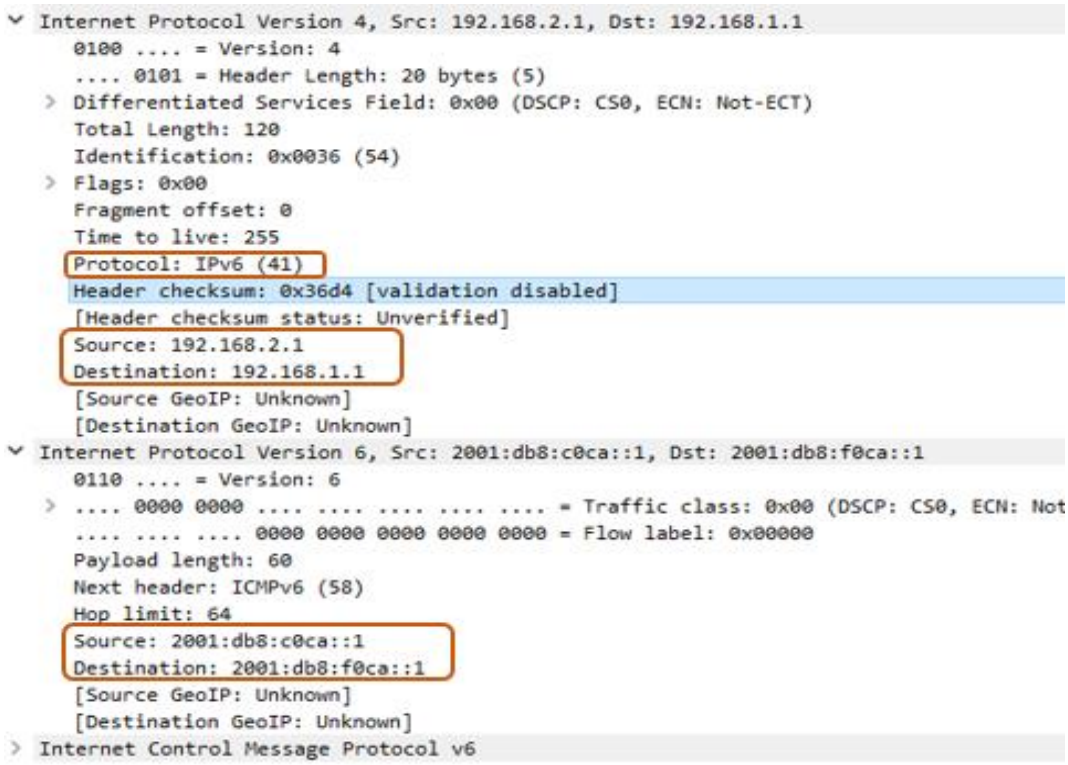


Figura 19. Resultado de análisis de túnel manual IPv6IP**.**

Las figuras 20, 21 y 22, se encuentran los gráficos de mapeo de tráfico de los túneles GRE, 6to4, ISATAP respectivamente donde se detalla la prueba de conectividad realizada de forma similar al grafico anterior.

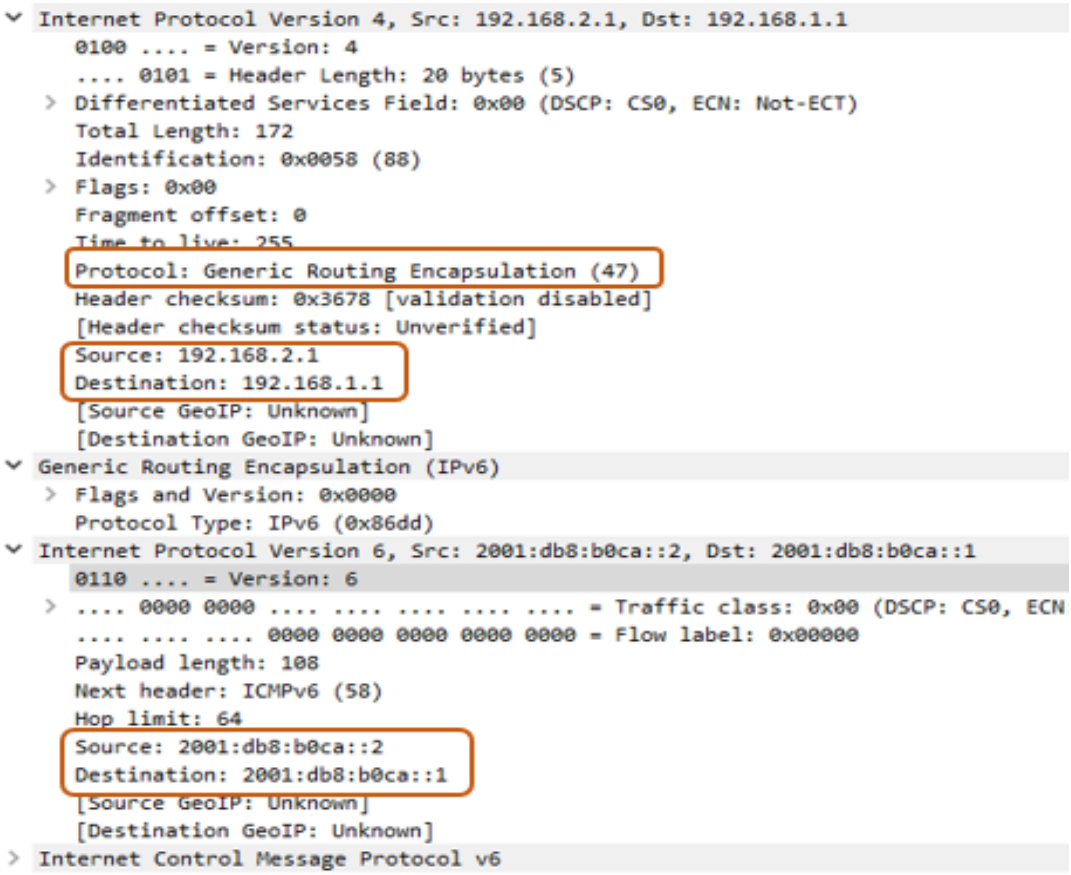


Figura 20. Resultado de análisis de túnel GRE

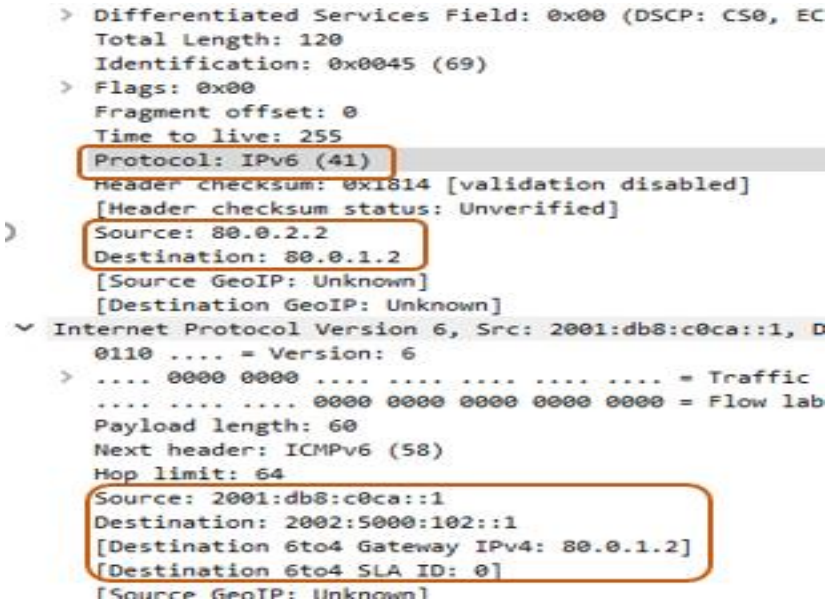


Figura 21. Resultado de análisis de túnel 6to4

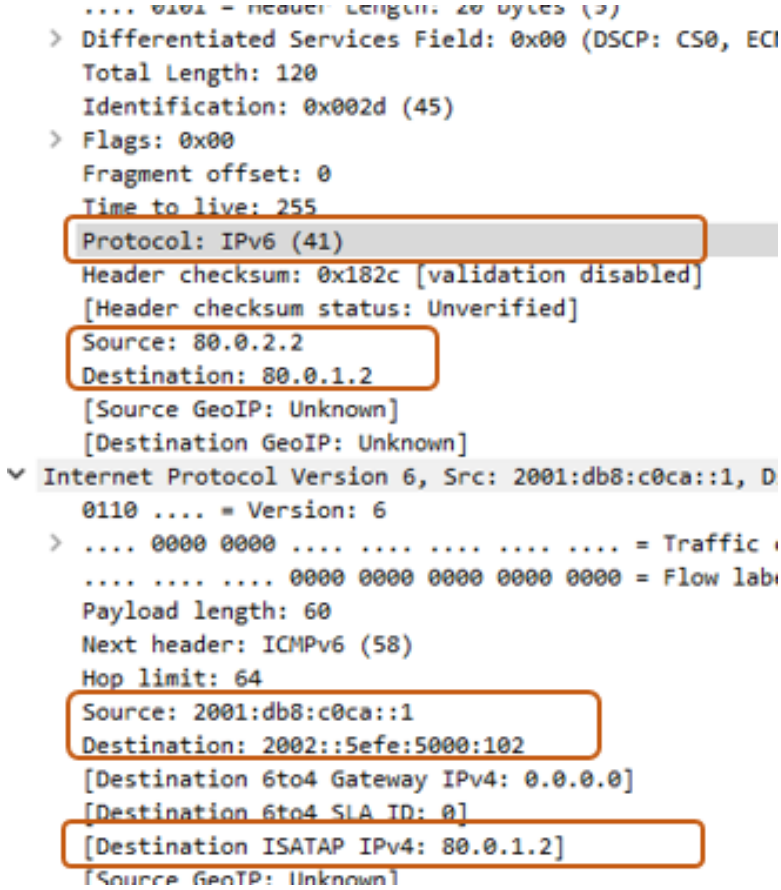


Figura 22. Resultado de análisis de túnel ISATAP

La Figura 23, muestra la forma como se envía el tráfico a través de la red con su respectiva encriptación para que no pueda ser alterada por terceras personas, la única información que se puede visualizar es el tipo de encriptación que se aplica al paquete, el origen y destino del túnel, pero no el origen y destino del paquete.

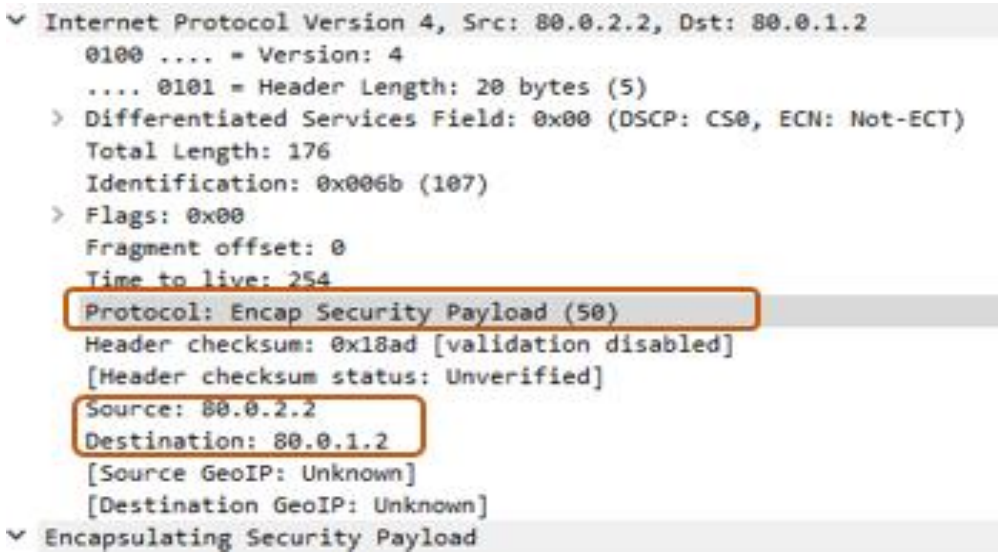


Figura 23.*Mapeo de tráfico del túnel GRE con Seguridad IP.*

La Figura 24, muestra la incompatibilidad con el tipo crypto profile de IPsec aplicada en un túnel manual.

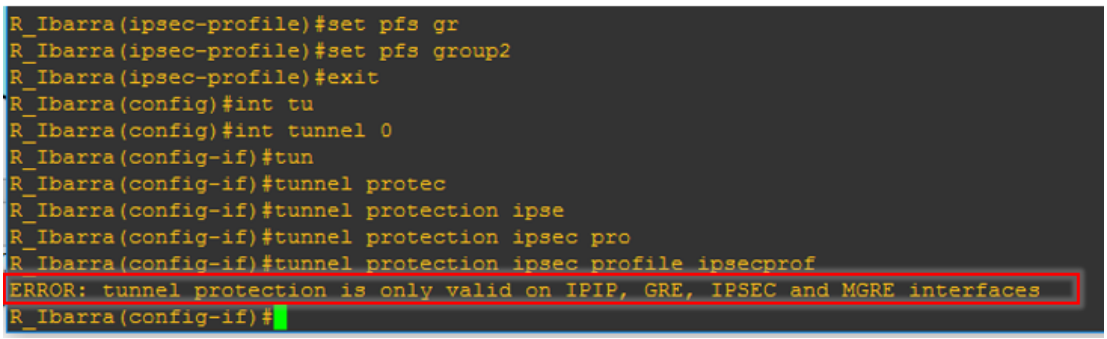


Figura 24. Archivo de configuración R_Ibarra muestra de incompatibilidad con profile IPsec.

4.2. DISCUSIÓN

De todos los túneles estudiados en la presente investigación aplicables para la transición entre las dos versiones del protocolo IP, los más estables, sencillos de configurar y el que tiene mejores opciones de seguridad a implementar fueron los túneles GRE compatibles con enrutamiento estático o dinámico, al igual que el transporte del tráfico de forma segura se lo implementa a través de la creación de perfiles que permiten implementar seguridad IPsec en la interfaz lógica del túnel creado, mientras que los otros túneles permite una seguridad por medio de la creación de mapas criptográficos que se aplican a la interfaz física del router y no son compatibles con la seguridad a través de perfiles criptográficos como muestra la figura 24.

La Tabla 9, muestra el análisis de las características y condiciones para un correcto enrutamiento aplicable a cada tipo de túnel y la seguridad aplicada.

Tabla 8. Características y condiciones para desarrollo de túneles IPv6

Túnel		**Área de uso**	**Enrutamiento**			**Condiciones**	**Seguridad IP**
			Estático	Ripng	OSPFv3		
Manual	**IPv6IP**	Punto a punto	X	X	X	Configuración debe conocerse en los dos extremos del túnel	Seguridad en tráfico IPv4 (crypto map)
	GRE	Genérico	X	X	X		Seguridad en túnel IPv6 (tunnel protection)
Automático	**6to4**	Puno - multipunto	X			Parte del direccionamiento debe contener embebida dirección IPv4	Seguridad en tráfico IPv4 (crypto map)
	ISATAP	Punto-multipunto	X			Dirección tipo EUI-64 tomando dirección IPv4 como parte de la dirección.	
	TEREDO	Túnel a través de NAT	X			Se utiliza detrás de dispositivos NAT.	

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Se recopiló información relevante para determinar los requisitos de una red en crecimiento de tipo empresarial, y cuáles son los ambientes que se pueden presentar para la implementación de túneles IPv6. Una vez determinados estos requisitos se logró concluir que el prototipo necesitó de redes LAN y enlaces WAN. El prototipo de la red fue simulado primero en el emulador GNS3 y aplicado en un ambiente controlado en el laboratorio de redes UTE.

Se utilizó el método analítico-sintético para el análisis y selección de las fuentes de información abordadas en la investigación y luego de la revisión de algunas metodologías se aplicó la metodología de diseño de redes Cisco PPDIOO para el desarrollo de toda la investigación, por brindar mayor flexibilidad y adaptabilidad a la presente investigación; con lo cual se logró una organización importante al seguir correctamente las fases y las actividades aplicadas cada una.

Se recreó la red LAN-WAN bajo los protocolos IPv4 para enlaces WAN y el protocolo IPv6 para las redes LAN, y su estructura de red contó con una red LAN principal que actúa como servidor y una sucursal donde se realizó la implementación de los clientes. Cabe mencionar que los túneles son una de las formas más viables para obtener conectividad y seguridad.

Se configuraron los equipos de Networking, servicios IPv6 virtualizados y se implementó seguridad IPsec cumpliendo el objetivo del proyecto que es conectividad a través de túneles IPv6. Realizando inicialmente pruebas en el

simulador GNS3 con los diferentes tipos de túneles explicados en la fase Operar de la metodología. Determinando con el cuadro comparativo establecido en la discusión del proyecto a el túnel GRE como el que más se ajusta a los requerimientos de nuestra red empresarial y aplicado a los dispositivos físicos en el laboratorio de redes de la UTE.

5.2. RECOMENDACIONES

Es recomendable elegir la metodóloga que más se ajuste a las necesidades del desarrollo del proyecto, que presente la flexibilidad necesaria en caso de realizar modificaciones en cada una de las fases en caso de tener que modificar los requerimientos y el alcance del proyecto.

Es recomendable conocer el funcionamiento del protocolo IPv6, sus tipos de direcciones, los servicios que este protocolo presenta y su estructura en general. Si no se tiene un fundamento teórico acerca de esta tecnología, es muy difícil poder llevar a cabo un proyecto de este tipo ya que pueden existir problemas en el momento de configurar e implementar un túnel.

Es recomendable usar herramientas de simulación de redes como GNS3 que es un emulador que se puede aplicar todas las configuraciones en un ambiente casi real, para analizar todos los posibles errores que se podrían presentar al momento de configurar los equipos físicos ahorrando un tiempo bastante considerable al momento de realizar configuraciones reales.

6. BIBLIOGRAFÍA

Ariganello, E., & Barriengos Sevilla, E. (2010). *Redes CISCO CNNP a fondo* (Primera ed.). Madrid, España: Alfa Omega RA - MA.

Beijnum, I. v. (2006). *IPv6 Running.* New York: Springer-Verlag New York,Inc.

Blanchet, M., Viangenie, & Parent, F. (2010). *IPv6 Tunnel Broker with the tunnel Setup Protocol.* IETF. Beon Solution. Obtenido de https://tools.ietf.org/html/rfc5572

Cicileo, G., Gagliano, R., O´Flaherty, C., Olvera Morales, C., Palet Martínez, J., Rocha, M., & Vives Martínez, Á. (2009). *IPv6 para Todos.* Buenos Aires: ISOC.Ar Asociación civil de argentinos en internet.

Cisco. (2007). *Implementing Tunnels.* Singapur: Cisco System Inc.

Cisco. (2012). *IPv6 Guia de Configuracion, Cisco IOS Realease 12.2SR.* Cisco.

Cisco. (2013). *Official Cert Guide CCNA Security &40-554.* (C. Press, Ed.) Indianapolis: Pearson Education, Inc. Obtenido de Cisco Networking Academy.

Cisco. (2015). *VPN Availability Configuration Guide, Cisco IOS Release 15M&T.* California: Cisco System, Inc.

Cisco. (2016). Ipv6 over Ipv4 GRE Tunnel Protection. En Cisco, *Security for VPN with IPsec configuration guide, Cisco IOS XE Release 3S* (pág. 14). San Jose: Cisco Systems, Inc.

Cisco, A. (2015). *Principios Básicos de enrutamiento y switching.* México: Academia Cisco.

Dave Evans. (2011). *Internet de las cosas como la proxima evolucion de internet lo cambia todo.* Cisco, Cisco Internet Business Solutions Group. Singapur: Cisco Systems, Inc.

Davies, J. (2012). *Understanding IPv6.* California: Microsoft Corporation.

Fierro, M. C., & Arrieta, V. (2015). Implementation of transition and coexistence mechanisms fot IPv4-IPv6 protocols. *Sistemas & Telematica*, 24.

Franciscone, H. (2009). *IPsec en ambientes IPv4 e IPv6* (Primera ed.). Guaymallen: Franciscone.

Hanumanthappa, J., & Manjaiah, D. H. (2009). IPv6 an IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model. *International Journal of Computer Science and Information Security, 3*(1), 12.

IBM. (Diciembre de 2016). *IBM Knowledge Center*. Obtenido de IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2/en/homepage.html

International Data Group. (15 de Abril de 2017). 5 Mitos del Internet of Things. (I. D. Group, Ed.) *Data Driven Business*, 68. Obtenido de computerworld.com.ec

IPv6TF-EC. (7 de Septiembre de 2009). *IP task force Ecuador.* Obtenido de IP task force Ecuador: http://ipv6tf.ec/

Jamhour, E., Storoz, S., & Maziero, C. (2003). Global Moovile IPv6 Addressing using transition mechanisms. *Graduate program in applied computer science, 8*(3), 14.

McCabe, J. D. (1997). *Practical Computer Network Analysis and Design* (2 ed.). San Francisco: Morgan Kaufmann.

Oracle. (2012). *Administración de Oracle Solaris: Servicios IP.* Oracle.

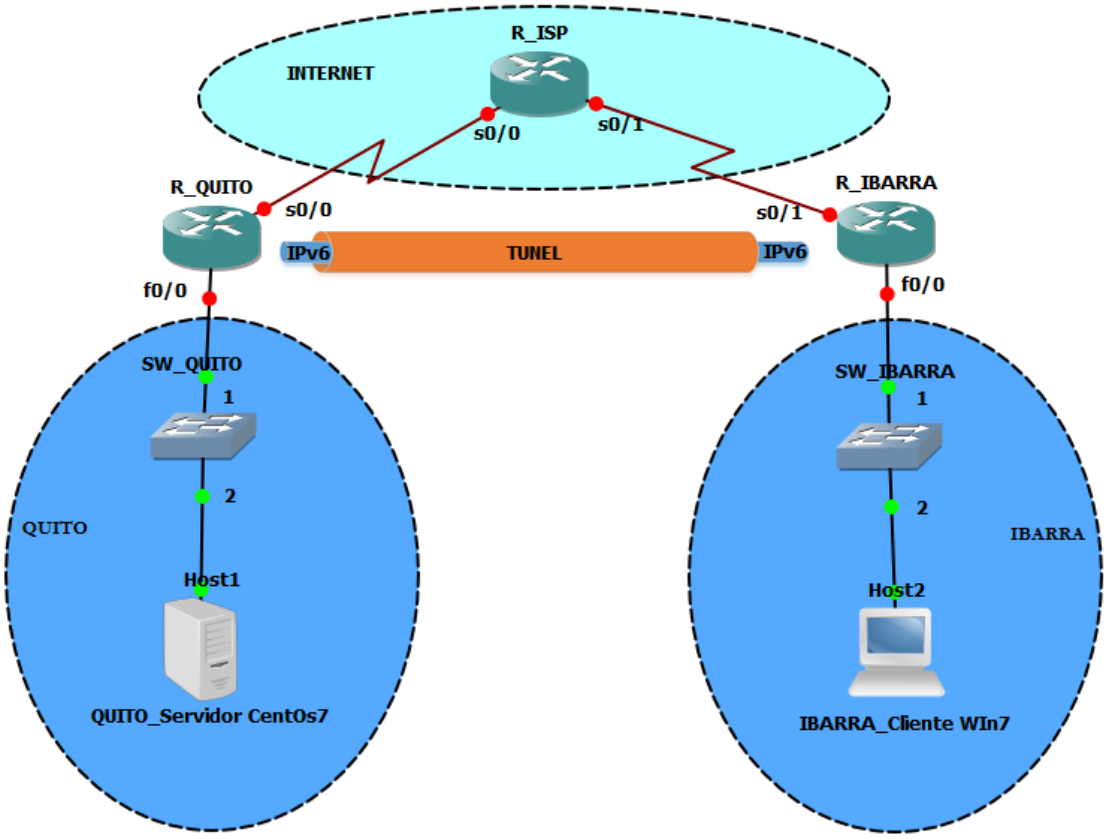
Priscilla Oppenheimer. (2011). *Top-Down Network Design* (tercera ed.). (Cisco, Ed.) Indianapolis: CiscoPress.

Stallings, W. (2004). *Comunicaciones y redes de computadores* (Séptima ed.). Madrid: Pearson Educacion, S.A.

Surf Net. (2013). *Preparing an IPv6 address plan.* Holanda: 2.

7. ANEXOS

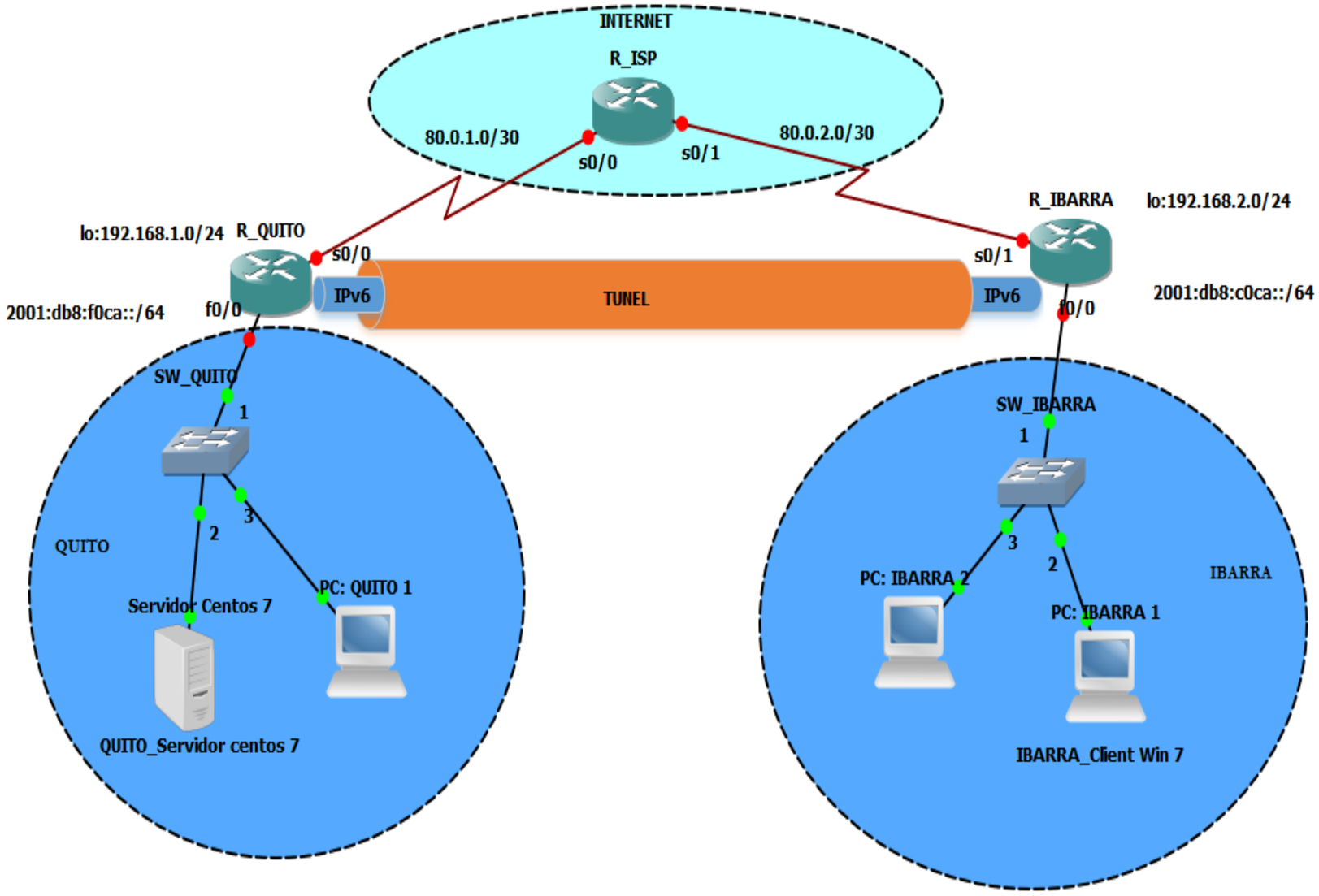
7.1. ANEXO 1. TOPOLODIA ESTRELLA



7.2. ANEXO 2. TABLA DE DIRECCIONAMIENTO

Dispositivo	Interfaz	Dirección IP	Prefijo
R_Quito	Fa0/0	2001:DB8:F0CA::1	/64
	S0/0	80.0.1.2	/30
	Tunnel 0	2001:db8:b0ca::1	/64
	Tunnel 1	2001:5000:102::1	/64
	Tunnel 2	2002:5000:102::1	/64
	Tunnel 3	2002:5FEE:5000:102::1	
R_Ibarra	Fa0/0	2001:DB8:C0CA::1	/64
	S0/1	80.0.2.2	/30
	Tunnel 0	2001:db8:b0ca::2	/64
	Tunnel 1	2002:5000:102::2	/64
	Tunnel 2	2002:5000:102::1	/64
	Tunnel 3	2002:5FEE:5000:102::1	/64
R_ISP	S0/0	80.0.1.1	/30
	S0/1	80.0.2.1	/30
Quito_Server	Fa0	2001:DB8:F0CA::10	/64
PC2_Quito	Fa0	2001:DB8:F0CA::3	/64
Ibarra_Client 1	Fa0	2001:DB8:C0CA::2	/64
Ibarra_Client 2	Fa0	2001:DB8:C0CA::3	/64

7.3. ANEXO 3. DIRECCIONAMIENTO IPV4 /IPV6



SIMBOLOGÍA

SERVER DIRECTO

CABLE

SWITCH

CABLE SERIAL

ROUTER

HOST

fecha: 20/03/2017	UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL
Dibujado por: Cristian Pozo	CONECTIVIDAD REMOTA CLIENTE SERVIDOR A TRAVÉS DE TÚNELES IPV6 Y SEGURIDAD IPSEC EN AMBIENTES MULTIPLATAFORMA.
Revisado por: Ing. Bolívar Jácome	