UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA: INGENIERÍA ELECTRÓNICA

Tesis previa a la obtención del título de:
INGENIERO ELECTRÓNICO

TEMA:
ANÁLISIS DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DEL PROTOCOLO IPSEC EN EL NODO DE INTERNET 2 DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO, CAMPUS SUR

AUTORA:
JOHANNA BERENICE ARGUERO TELLO

DIRECTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, noviembre de 2013

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Yo Berenice Arguero autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de la autora.

Johanna Berenice Arguero Tello
CC: 1723989149

DEDICATORIA

A Dios, a mi familia querida, a mis padres por brindarme su apoyo incondicional, por haberme dado el regalo más valioso, mi profesión; a mi madre por creer en mí y estar a mi lado en los días que más le he necesitado. A mis hermanos que han estado ahí siempre, gracias por su apoyo y sacar una sonrisa de mi rosto cuando he estado agotada por el día de trabajo. También dedico este proyecto a esa persona especial, mi compañero inseparable de cada jornada. Quien me animaba en aquellos momentos de decline y cansancio.

A mis amigos por los buenos y malos momentos que vivimos dentro y fuera de nuestro centro de estudio, este trabajo lo he realizado con su apoyo incondicional.

AGRADECIMIENTO

Mis más sinceros y profundos agradecimientos a aquellas personas que de una u otra manera han colaborado con los resultados de este proyecto, especialmente está dirigido a mi tutor de tesis Ing. Jorge López, quién con sus conocimientos y ayuda incondicional supo guiarme en el camino del saber.

A mis profesores a quienes les debo gran parte de mis conocimientos, gracias a su paciencia, enseñanza y finalmente un eterno agradecimiento a esta prestigiosa universidad la cual abre sus puertas a jóvenes como nosotros, para prepararnos para un futuro competitivo y formarnos como buenos cristianos y honrados ciudadanos.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

La red académica avanzada conocida como Internet 2, aporta a promover y optimizar los procesos formativos en la educación superior, la generación de conocimiento y la creación de nuevas tecnologías, esto se lleva a cabo mediante el desarrollo de ciertas aplicaciones sobre esta plataforma, inclusive la Universidad Politécnica Salesiana Sede Quito Campus Sur, se encuentra en fase de desarrollo de prototipos además de proyectos en el área de la Telemedicina; en este aspecto el presente documento hace referencia a brindar seguridad a esta red con el empleo de protocolo IPSec con el fin de poner en marcha los prototipos y proyectos.

A diferencia de otros protocolos, este ofrece una solución a la seguridad transparente para el usuario a su vez posee mecanismos de autenticación y confidencialidad independientemente de las aplicaciones que se emplee. Para la implementación de dicho protocolo se realizó un estudio analítico dentro de un escenario de simulación para redes conocido como GNS3 apoyado en la herramienta Wireshark, arrojando cifras tales como: el número de paquetes transportados, el tiempo de transmisión dado que son factores que determinan sí, es factible realizar la implementación del protocolo se seguridad IPSec en la red de Internet 2 en la UPS.

ABSTRACT

The advanced academic network known as Internet 2, brings to promote and optimize the learning processes in higher education, the creation of knowledge and the creation of new technologies, this is done by developing some applications on this platform, including Salesian University South Campus is in prototype development phase as well as projects in the area of telemedicine and in this respect the present document refers to providing security to the network with the use of IPSec protocol in order to make prototypes and production projects.

Unlike other protocols, this provides a solution to the security transparent to the user in turn holds authentication and confidentiality mechanisms irrespective of the applications being used. For the implementation of this protocol was performed an analytical study in a simulation scenario known as GNS3 networks supported by Wireshark tool , throwing figures such as the number of packages shipped , the transmission time as other factors that determine it is feasible to implement the IPSec security protocol on the Internet 2 in the UPS .

INTRODUCCIÓN

La red académica avanzada en el Ecuador está bajo el cargo del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado conocido como CEDIA cuyos propósitos están enfocados al desarrollo científico, tecnológico, innovador y educativo, conformado por universidades, centros de investigación a nivel nacional y a su vez está asociada a la Red CLARA a nivel de América Latina para una interconexión mundial.

Las aplicaciones de Internet 2 se encuentran en fase de desarrollo, revolucionando la comunidad científica, en aplicaciones como: laboratorios virtuales, bibliotecas virtuales, tele-presencia, telemedicina, telecontrol, etc. Cabe considerar, por otra parte que en la Universidad Politécnica Salesiana Sede Quito, Campus Sur se encuentran desarrollando aplicaciones para la red avanzada de la universidad, sin embargo estos prototipos han sido manipulados por terceras personas, modificando sus características.

En vista de la falta de protocolos de seguridad para la red de Internet 2, no se ha podido poner en marcha dichas aplicaciones tanto para el desarrollo educativo como tecnológico.

De las evidencias anteriores se busca solucionar la seguridad de la red con la implementación del protocolo de seguridad IPSec en el diseño tanto físico como lógico propuesto dentro de un escenario de simulación GNS3. En primer lugar se realizará un análisis de la arquitectura del protocolo IPSec con el propósito de elegir que protocolo se utilizará finalmente, en virtud de la herramienta conocida como Wireshark, se realizará un análisis analítico y comparativo entre dos escenarios de estudio para determinar el número de paquetes transmitidos y el tiempo de transmisión de dichos paquetes, ya que serán indicadores para señalar que es factible implementar IPSec en la red de Internet 2 de la UPS como una solución a la seguridad.

CAPÍTULO 1
PLANTEAMIENTO DEL PROBLEMA

1.1 Planteamiento del problema

Los prototipos o demos que se encuentran desarrollando para la red avanzada de la Universidad Politécnica Salesiana Sede Quito Campus Sur, no han sido puestos en práctica, ya que estos de una u otra forma han sido manipulados, modificando sus características por terceras personas en vista de la falta de protocolos de seguridad para dicha red.

1.2 Hipótesis

"Es factible la implementación del protocolo de seguridad IPSec, para el mejoramiento de la seguridad del nodo de Internet 2 de la Universidad Politécnica Salesiana Sede Quito Campus Sur".

La seguridad es un punto destacado en los requerimientos de una red, la misma que va a depender de las aplicaciones que trabajan en su entorno, motivo por el cual el brindar seguridad a nivel de capa de red garantizará que el tráfico procesado por los protocolos de niveles superiores se comuniquen de manera segura y protegida, una de las maneras más eficientes de lograr este cometido es mediante el uso del protocolo de seguridad IPSec, el mismo que entre sus principales características posee la capacidad de gestionar el intercambio de claves compartidas para cifrar y autenticar el origen de los datos.

1.3 Objetivos

1.3.1 Objetivo General

Realizar un análisis de factibilidad para la implementación del protocolo IPSec para el Nodo de Internet 2 de la Universidad Politécnica Salesiana Sede Quito Campus Sur.

1.3.2 Objetivos Específicos

- Realizar un análisis de la arquitectura del protocolo IPSec.
- Realizar un levantamiento de la situación inicial de la red de Internet 2 de la UPS Campus Sur.
- Generar una propuesta de implementación del protocolo IPsec por medio de la simulación del entorno de red bajo investigación.

CAPÍTULO 2
ESTADO DEL ARTE

Uno de los requerimientos de la red es ofrecer seguridad, de hecho en el entorno de Internet 2 la falta de seguridad puede ser un problema dado que se maneja información de alta importancia y criticidad. Es así que el implementar seguridad a nivel de la capa de red brinda integridad de la información, en vista que el paquete debe ser transmitido de un punto a otro de manera protegida.

El protocolo de seguridad de internet conocido como IPSec, proporciona seguridad a nivel de capa red y a los protocolos de niveles superiores, cumpliendo con el objetivo de autenticar e encriptar la información que se quiere transmitir, por su parte se han realizado estudios respecto a la implementación del protocolo de seguridad IPSec tanto en infraestructuras comerciales como en infraestructuras de redes avanzadas, entre otros se puede mencionar algunas de ellas:

- Mendoza Ma. Concepción y Covarrubias David en su trabajo llamado "IPSec una alternativa para brindar seguridad para Internet 2 en México", menciona que el protocolo IPSec puede ser empleado en cualquier contexto; sin embargo su implementación estará definida por los requerimientos de seguridad de la red, por lo que anuncian que el protocolo de seguridad protege además los protocolos de alto nivel, es así que puede proteger cualquier tipo de tráfico transportado sobre IP. El objetivo de estudio fue evaluar el protocolo IPSec en el ambiente de Internet 2 en México y como escenario de experimentación se realizó en una infraestructura de Internet 2, establecieron túneles de conexión con dos instituciones académicas con la finalidad de validar la interoperabilidad de implementación IPSec sobre IPv6. Por lo tanto se validó la protección de la transmisión de la información, indicando que hubo un diferencia significativa entre la información visible de los paquetes trasportados una vez empleado la VPN, como obtuvo como resultado información encriptado valorando así la aplicación del protocolo de encriptación. (2002, pág. 1-11)

- En el artículo publicado en septiembre del 2008 llamado “IPSec de IPv6 en la Universidad de Pamplona”, por los autores Rico Dewar, Mediana Yurley y Santos Luz Mariana, mencionan una vez culminado con su trabajo, que se puede realizar conexiones seguras mediante el protocolo IPSec en ambientes IPv6, a través del uso de logaritmos de encriptación; de esta manera se asegura la confidencialidad y la autenticación de la información al ser transmitida. Incluso indican que el uso de este protocolo puede causar una desmejora en el desempeño de la red. De hecho este protocolo debe ser empleado especialmente cuando se tiene que proteger a todo el tráfico caso contrario no es necesario implementarlo.(pág. 325)

- Santiago Pérez, en su artículo “Análisis del protocolo IPSec: el estándar de seguridad en IP”, hace un análisis acerca de los servicios de seguridad que brinda el protocolo IPSec, tales como: integridad y autenticación de origen de datos, confidencialidad, detección de repeticiones, el control de acceso y el no repudio los cuales en conjunto garantizan una protección de la información.

  Al hablar de protección de la información en especial a nivel de capa red, el autor menciona que brinda una gran ventaja, debido a que ofrece una seguridad homogénea, independientemente de la aplicación, siempre y cuando estén basadas en IP. Para esto se requiere especificar el tipo de escenario donde se implementará IPSec, y así determinar la solución más viable observando sus ventajas de IPSec sobre ellas.

  Menciona tres tipos de escenarios que son: Interconexión segura de redes locales, acceso seguro de usuarios remotos y conexión de una corporación con los proveedores.
  La interconexión segura de redes locales o conocida como intranet, se encuentra basada en una infraestructura que puede ser pública o privada donde se conecta todos los puntos de trabajo empleando Gateways IPSec,

como ejemplo para este escenario se tiene las instituciones bancarias donde requieren un alto nivel de protección por lo que es factible la implementación de IPSec.

Cambiando de escenario, está el acceso seguro de usuarios remotos, donde se requiere acceder de forma segura a la información desde cualquier parte del mundo. Menciona que el uso de este protocolo garantiza confidencialidad y autenticación de una comunicación de extremo a extremo. Por lo tanto IPSec cumple con el perfil de seguridad que requiere una comunicación remota. Finalmente está la extranet donde interconecta una central con sus sucursales, IPSec ofrece una ventaja frente a otras soluciones dado que se pueden conectar de forma segura sin importar el equipo que se utilice, ya que es una tecnología avanzada con estándares internacionales logrando así la interoperabilidad. Para ello emplea Gateways IPSec en cada uno de los puntos de presencia de la extranet. (2001, pág.60-61)

La UPS Sede Quito Campus Sur, se encuentran desarrollando proyectos para aplicar en la red de Internet 2, sin embargo no han podido ser puestos en práctica por no contar con la seguridad correspondiente para la red; por lo tanto el análisis de propuesta para la implementación del protocolo de seguridad IPSec, dependerá de: el escenario de implementación y de lo que se quiera proteger. Esta puede ser una comunicación de extremo a extremo o realizar una protección sin incluir a los dispositivos intermedios para construir una solución de seguridad más adecuada para garantizar seguridad de transmisión de información en una comunicación.

CAPÍTULO 3
MARCO TEÓRICO

3.1 Internet 2

Es la interconexión de universidades, institutos, centros de investigación de alta velocidad para la interacción de la comunidad científica, fundamentada en el diseño y desarrollo de nuevas aplicaciones y tecnologías de red con el objetivo de crear la infraestructura de comunicación de altas prestaciones del futuro (Rallo & Gisbert, 2002, pág. 7).

Internet 2 es conocida como red académica avanzada, que comparte grandes flujos de información, difusión de tecnología, además de facilitar la coordinación de grupos de trabajos a largas distancias, permitiendo desarrollar proyectos de investigación científica para promover y optimizar los procesos formativos en la educación superior y la generación de conocimiento en el ciberespacio sin poseer las limitantes que presenta el internet comercial, como es el ancho de banda, el cual es mayor en comparación al internet convencional, y con un tiempo de acceso es más reducido debido al nivel de la infraestructura.

Esta red se encuentra aún en fase de desarrollo y cuyas aplicaciones se encuentran basadas en la computación distribuida o grid, permitiendo compartir los recursos que están distribuidos geográficamente brindando control y monitoreo de las diferentes aplicaciones que la empresa o institución lo requiera a largas distancias. Gracias a la tecnología middleware permite la interoperabilidad en los recursos compartidos, el acceso a la información y la gestión para un correcto funcionamiento de dichas aplicaciones sobre esta plataforma.

A continuación se menciona algunas aplicaciones que están revolucionando con este tipo de tecnología en el mundo educativo y científico, las cuales son:

- Laboratorios virtuales, con lo cual se puede acceder desde cualquier parte del mundo, logrando manipular y obtener datos desde su computador personal.

- Bibliotecas digitales que permite obtener: libros, artículos, periódicos en formato digital, además de videos educativos en alta definición.

- Telemedicina, prestando servicios médicos tales como: consulta, diagnósticos, cuidado, radiología, patología, cardiología, endoscopia, cirugía o realizar un monitoreo de los signos vitales desde puntos geográficos remotos para la población que no tenga acceso a los servicios médicos.

- Tele-presencia o Tele-inmersión, que se basa en el uso de interfaces de usuario para crear la sensación de co-presencia trabajando en escenarios virtuales. (Rallo & Gisbert, 2002, pág. 11)

- Learnigware, es un software educativo donde su misión es la educación remota o a distancia ya sea tanto en tiempo real como diferida.

- Realidad virtual, un mundo virtual generado por ordenador con el que se puede interactuar con los objetos presentes dentro de un escenario virtual.

- Telecontrol, con esta aplicación permite manipular, controlar a los dispositivos electrónicos remotamente, específicamente en el campo de la robótica, domótica.

3.1.1 RedCLARA

En Latinoamérica la interconexión de las redes académicas está dada por la RedCLARA, y esta a su vez se interconecta mundialmente con la red GÉANT2 en Europa, INTERNET2 en Estados Unidos, APAN en Asia.

La interconexión con la red europea GÉANT2 lo hace a través del enlace en Brasil con el Punto de presencia (PoP) en Sao Paulo, hasta el punto de acceso en Madrid (España) con una velocidad de 622Mbps; con este enlace la RedCLARA también accede a la zona Asia-Pacífico y al Mediterráneo debido a que la Red GÉANT2

posee enlaces a las redes TEIN2 (Trans-Eurasia Information Network) y EUMEDCONNECT correspondientemente.

Con Estados Unidos, se conecta mediante dos enlaces uno en Brasil con el PoP Sao Paulo(SAO) hacia el PoP AtlanticWave y el segundo en México con el Pop Tijuana(TIJ), que se enlaza hacia el PoP de PacificWave con una velocidad en su enlace de 1Gbps. Este Punto de Presencia permite acceder a las conexiones hacia el Asia-Pacífico, a la red APAN (Red Avanzada del Asia-Pacífico). Debido que se ubicada en la ciudad de San Diego en las costas de Estados Unidos.

3.1.1.1 Países Asociados a la RedCLARA

Los países asociados a la RedCLARA, deben estar conectados a la Red Nacional de Investigación y Educación conocido como RNIE, y a su vez son miembros de la RedCLARA. Actualmente los países latinoamericanos que se encuentran interconectados a la RedCLARA son los mencionados a continuación con su respectivo nombre de la red proporcionados por el sitio web de la RedCLARA.

- Argentina, INNOVARED
- Brasil, RNP
- Colombia, RENATA
- Costa Rica, CR2Net
- Chile, REUNA
- Ecuador, CEDIA
- El Salvador, RAICES
- Guatemala, RAGIE
- México, CUDI
- Nicaragua, RENIA
- Panamá, RedCyT
- Paraguay, Arandu
- Perú, RAAP
- Uruguay, RAU

- Venezuela, REACCIUN (RedCLARA, 2012)

3.1.1.2 Servicios de la RedCLARA

Los servicios que ofrece la RedCLARA a la comunidad científica, para el desarrollo de la educación, investigación a nivel mundial, son los siguientes:

- IPv4 / IPv6
- Multicast
- Multicast IPv6
- Disponibilidad de Ancho de Banda (QoS)
- Mediciones
- Servicios específicos para proyectos: Mallas Computacionales (Grids)

Adicionalmente presta servicios de apoyo a la colaboración para la red tales como:

1. **SIVIC - Multiconferencia**

   Este servicio se compone de unidades de videoconferencia multipunto para maximizar la interacción de la comunidad de investigación y en el desarrollo regional, así se puede integrar varias videoconferencias que se encentran en diversos países pero dentro de un mismo espacio. (RedCLARA, 2012).

2. **VC Expreso**

   Es un servicio de videoconferencia exclusivo, donde la comunicación es en tiempo real, sin las limitantes en el tiempo de uso, ni el número de usuarios conectados dentro de su comunidad. (RedCLARA, 2012).

3. **Videos a Pedido o Video en Demanda**

   Es una plataforma que contiene un amplio catálogo de videos de múltiples áreas del conocimiento como: capacitaciones técnicas en el tema de la implementación de nuevos servicios y aplicaciones para el Internet 2. (RedCLARA, 2012)

4. Albergue de videos

Brinda la facilidad de albergar videos elaborados por la comunidad científica, en la plataforma de videos a pedido, sin ningún valor económico. (RedCLARA, 2012)

5. Alerta de fondos de financiamiento

Ofrece al usuario recibir información de apertura de fondos de financiamiento en áreas de preferencia a través del portal personal. (RedCLARA, 2012)

6. Alerta de Evento

Es una aplicación de aviso para indicar fechas a eventos científicos y académicos para las comunidades de investigación latinoamericanas. (RedCLARA, 2012).

7. eScaparate

Es un servicio exclusivo de los miembros de la RedCLARA, que hospeda páginas Web para comunidades científicas latinoamericanas, brindando la oportunidad de exponer los proyectos, investigaciones, publicaciones de los avances y resultados de investigación, fotografías y más. Cuenta con características relevantes tales como:

- Disponibilidad de 24 horas y los 365 días del año.
- Tráfico ilimitado.
- Acceso remoto vía FTP (de uso exclusivo para el organizador).
- Publicación en el dominio http://.redclara.net/.
- Acceso directo desde la página de inicio de la comunidad, dentro del Portal de RedCLARA.
- Disponible para la publicación de información institucional en formato Web basado en HTML estándar.
- No permite la instalación de bases de datos o aplicaciones ad hoc. (RedCLARA, 2012)

Con el fin de mantener un alto rendimiento en la operación y brindar una alta disponibilidad en los servicios avanzados que presta la red académica, existe un Comité Técnico, el cual debe proveer la mejor información y el más alto flujo de comunicaciones entre los grupos, protegiendo así, aquellos asuntos técnicos y políticos de los miembros de RedCLARA (RedCLARA, 2012). Para desempeñar esta función depende tanto del Centro de Operaciones de la Red como en el área de ingeniería de la red está el Grupo de Ingeniería de la Red y el Grupo de Ingeniería de Sistemas.

La RedCLARA indica que el Grupo de Ingeniería de la Red conocido como NEG, se encuentra a cargo de la arquitectura y la ingeniería de la RedCLARA, preocupándose por el diseño, la planificación y el desarrollo de la dicha red; esto es posible ya que se encarga de puntos importantes como son:

- Consolidar los acuerdos de intercambio de tráfico con las Redes Académicas de Asia-Pacífico y Europa Oriental.
- Analizar la seguridad de RedCLARA.
- Diseñar el conjunto de indicadores básicos de calidad de RedCLARA.
- Llevar a cabo análisis de tráfico.
- Desarrollar e implementar calidad de servicio en RedCLARA (QoS).
- Planificar e instalar nuevas redes nacionales conectadas a RedCLARA.
- Establecer los mecanismos de operación de un servidor de videoconferencias (VC). (RedCLARA, 2012)

Con la finalidad de mejorar la operación, los servicios, y las características técnicas, el NEG realiza las siguientes funciones:

- Definir Plan de Servicios 2008-2012.
- Determinar necesidades de ancho de banda.
- Establecer recursos de transporte disponibles.
- Desarrollar el Plan Técnico.
- Discutir la Estrategia Técnica con las Redes Nacionales.

- Discutir la Estrategia Técnica con las instituciones aliadas.
- Desarrollar en concordancia con el Plan de Ingeniería así construido, el Proyecto RedCLARA2 para la propuesta de ALICE2.
- Implementar las primeras etapas de la red óptica de RedCLARA. (RedCLARA, 2012)

El Centro de Operaciones de la Red conocido por sus siglas NOC, cumple el papel fundamental de la administración, el control, el monitoreo, y operación diaria de todas las infraestructuras que conforman la RedCLARA tanto de la parte física como lógica, para asegurar así un alto rendimiento en la operación de la red. Esta entidad está dirigida por la Red Universitaria Nacional REUNA que se encuentra ubicado en la ciudad de Santiago de Chile entregando los servicios de mantenimiento correctivo en la modalidad 7x24 es decir los siete días de la semana y las veinticuatro horas del día. (RedCLARA, 2012).

El Grupo de Ingeniería de Sistemas o llamado SEG, es el agente de la administración de los servidores además proporcionar seguridad en los sistemas que se encuentran en la red, asimismo es el encargado de dirigir los sistemas, las aplicaciones y el software que corre por toda la red. Este grupo desempeña dos funciones esenciales: la operación de sistemas de monitoreo y la prevención de riesgos y seguridad. Para lograr cuyo objetivo la RedCLARA realiza las siguientes funciones:

- Diseño e implementación de sistemas de herramientas de monitoreo.
- Mantener contacto con las RNEI y el NOC para solucionar sus problemas de servicios.
- Mantenimiento de servidores y hardware.
- Mantenimiento de software (OS y aplicaciones).
- Instalación de nuevas aplicaciones y servicios.
- Administración de respaldos y riesgos.
- Prevención de seguridad.
- Respuesta a incidentes de seguridad.

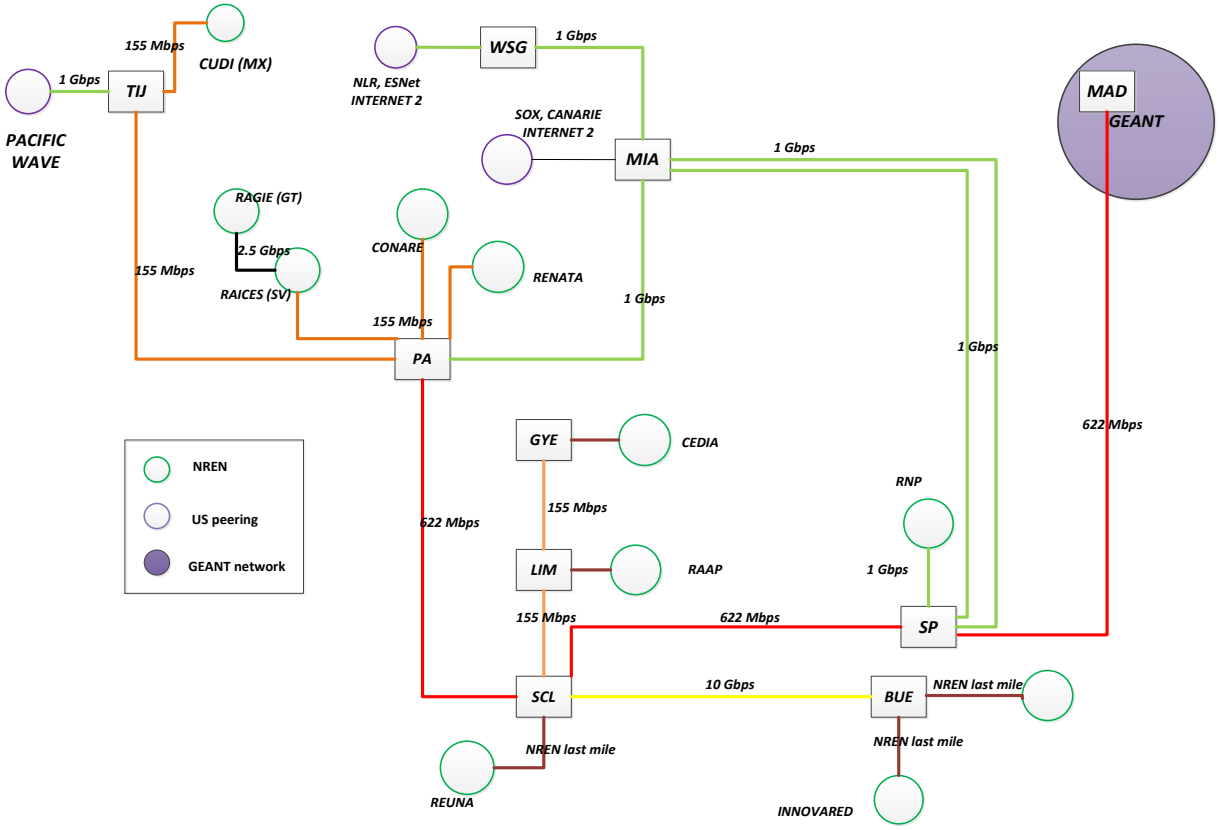
- Reportes (RedCLARA, 2012).

3.1.1.3 Descripción Técnica de la RedCLARA

El backbone de la RedCLARA está compuesto por diez nodos ruteadores principales, conectados en una topología punto-a-punto. En la figura 1 se identifica la conexión de los nodos, donde cada uno de ellos representa a un punto de presencia conocido por sus siglas PoP; estos puntos de presencia representan la ubicación física de los equipos activos como los routers, switches, servidores para lograr tener el acceso al internet, La RedCLARA está formado por los siguientes PoP´s:

- **MIA** (Miami - Estados Unidos)
- **SAO** (Sao Paulo - Brasil)
- **BUE** (Buenos Aires Argentina)
- **SCL** (Santiago de Chile - Chile)
- **LIM** (Lima - Perú)
- **GYE** (Guayaquil - Ecuador)
- **BOG** (Bogotá - Colombia)
- **PTY** (Panamá - Panamá)
- **TIJ** (Tijuana - México)
- San Salvador (El Salvador) (RedCLARA, 2012)

Figura 1 Topología de la RedCLARA, Julio 2011



Fuente: RedCLARA

3.1.2 Red CEDIA

La red CEDIA es el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, fue creada para estimular, promover y coordinar con el Proyecto Redes Avanzadas, el desarrollo de las tecnologías de información, las redes de telecomunicaciones e informática enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador. (CEDIA, 2012).

Actualmente CEDIA está conformado por universidades, institutos superiores, centros de investigación y por departamentos gubernamentales a nivel nacional, cuyos miembros académicos, miembros honorarios y miembros estratégicos se mencionan a continuación:

1. **Miembros Académicos**

   Escuela Politécnica del Ejército - ESPE

   Universidad Estatal de Milagro UNEMI

   Escuela Politécnica Nacional - EPN

   Universidad Internacional del Ecuador - UIDE

   Escuela Superior Politécnica del Chimborazo - ESPOCH

   Universidad Técnica de Ambato. UTA

   Escuela Superior Politécnica del Litoral - ESPOL

   Universidad Nacional de Chimborazo - UNACH

   Instituto Oceonográfico de la Armada - INOCAR

   Universidad Nacional de Loja - UNL

   Pontificia Universidad Católica del Ecuador Sede Ibarra - PUCESI

   Universidad Politécnica Salesiana - UPS

   Pontificia Universidad Católica del Ecuador Sede Quito - PUCE

   Universidad Regional Autónoma de los Andes - UNIANDES

   Pontificia Universidad Católica Sede Santo Domingo - PUCESD

   Universidad San Francisco de Quito – USFQ

   Secretaría Nacional de Educación Superior,Ciencia, Tecnología e Innovación – SENESCYT

   Universidad Técnica del Norte - UTN

   Universidad Católica de Santiago de Guayaquil - UCSG

   Universidad Técnica Particular de Loja - UTPL

   Universidad Central del Ecuador - UCE

   Universidad Tecnológica Equinoccial - UTE

   Universidad de Cuenca - UC

   Universidad Estatal de Bolívar – UEB

   Universidad Tecnológica Indoamérica - UTI

   Instituto de Altos Estudios Nacionales – IAEN

2. **Miembros Honorarios**

   Steve Hurter, Universidad de Oregon, Carlos Monsalve (ESPOL), Enrique Peláez (ESPOL)

3. **Miembros Estratégicos**

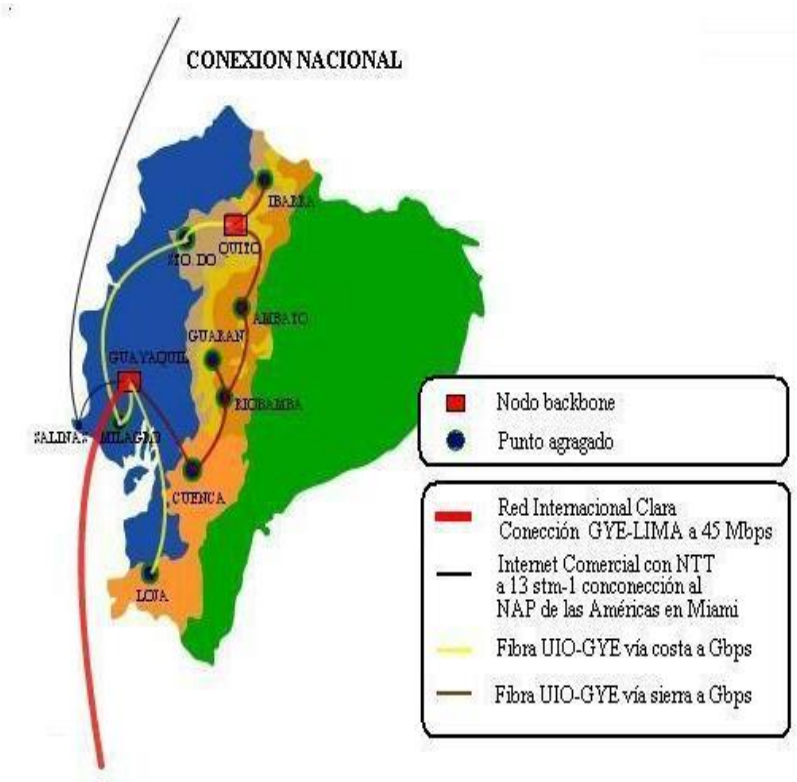
   Compañía Nacional de Transmisión Eléctrica

   Consejo Nacional de Telecomunicaciones (CEDIA, 2010)

3.1.2.1 Descripción Técnica de la Red

La Red CEDIA está formada a nivel nacional por un anillo de fibra óptica, que interconecta a las ciudades de Ibarra, Quito, Ambato, Riobamba, Guaranda, Cuenca, Guayaquil, Loja y Santo Domingo a una velocidad de transmisión de 1Gbps, para todos sus miembros a través del proveedor de servicios TELCONET. En la figura 2 se indica cómo se encuentra realizada la conexión nacional de la red CEDIA.

Figura 2 Conexión Nacional de la red CEDIA



Fuente: CEDIA

Este anillo emplea la tecnología MPLS (MultiProtocol Label Switching),es un estándar de la IETF publicado en el RFC3031; esta tecnología orientada a conexión tiene la capacidad de soportar múltiples protocolos brindando: calidad de servicio Qos, ingeniería de tráfico y redes privadas virtuales, con estas características

mencionadas se reduce el procesamiento del paquete que ingresa al enrutador, al trabajar a nivel de capa 2 y capa 3 del Modelo OSI, permite conmutar y enrutar basándose en el valor de la etiqueta que se añade en el paquete, mejorando así el desempeño y la optimización de la red.

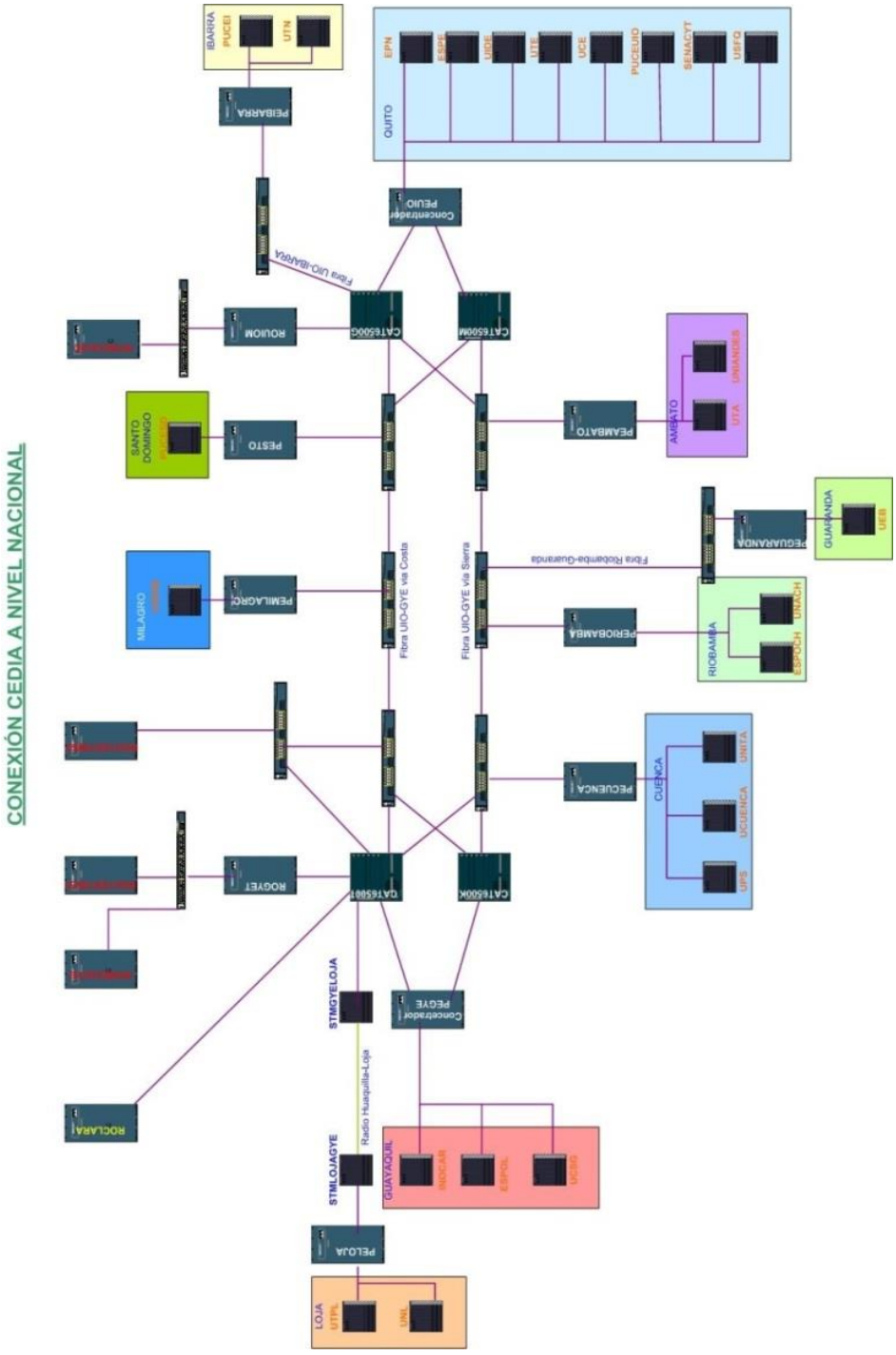
3.1.2.2 Topología de la Red CEDIA

Los dispositivos activos que utiliza la Red CEDIA, son de la marca Cisco de alto rendimiento, brindando confiabilidad en la transmisión de información, un tiempo de servicio alto; por otro lado posee ventajas muy claras con respecto a aquellas instituciones que no forman parte de la red CEDIA (CEDIA, 2010); se puede apreciar en la figura 3 que el 99,9% de la red a nivel nacional se maneja con fibra óptica exceptuando el enlace Huaquillas-Loja, ya que este es por radio. Adicionalmente tiene dos arterias principales redundantes que interconecta las diferentes instituciones, estos enlaces son: Quito-Guayaquil vía Costa, y el enlace Quito-Guayaquil vía Sierra.

La conexión hacia la RedCLARA se realiza mediante un switch de borde Catalyst 6500T, el cual está ubicado en la provincia de Loja.

El acceso hacia la red avanzada de la UPS de la ciudad de Quito es mediante el punto de acceso en la ciudad de Cuenca desde la Sede Quito este tiene el acceso por el ramal sierra Quito-Guayaquil por fibra óptica.

Figura 3 Topología Lógica y Física de la Red CEDIA



Fuente: CEDIA

3.2 Situación Actual de la Red de Datos de la UPS, Campus Sur

La Universidad Politécnica Salesiana Sede Quito Campus Sur, perteneciente a una congregación salesiana sin fines de lucro, presta los servicios que se mencionan a continuación:

- Ambiente Virtual de Aprendizaje Cooperativo (AVAC), el cual es una herramienta de e-learning y multimedia, basada en el Internet.
- Bibliotecas Virtuales, el cual contiene una base de datos que funciona como una biblioteca virtual formada por: publicaciones, revistas, libros además se encuentra vinculada con bibliotecas virtuales contratadas por la UPS.
- Servicios de Video Conferencia
- Portal WEB
- VOIP
- Laboratorios
- Publicaciones
- Centros de Investigación
- Internet 2

En el Campus Sur, se incluye especialmente dos Centros de Investigación, conocidos por sus siglas CIMA y CIVABI, por lo que las aplicaciones de cada centro de investigación necesitan otros tipos de requerimientos que no ofrece el internet comercial, de hecho el empleo de Internet 2 es el mejor aliado para dichas aplicaciones.

CIMA (Centro de Investigación en Modelamiento Ambiental)

El centro de investigación tiene como objetivo dar respuestas científicas a las necesidades de gestión ambiental, convirtiéndose en un referente nacional en cuanto el estudio del ambiente, generando información accesible, confiable y oportuna que permita la generación de planes a nivel local, nacional e internacional para su cuidado y preservación; es así que la misma maneja las siguientes líneas de investigación:

- Estudio del clima y tiempo
- Análisis de señales sísmicas
- Ecología, Recursos Naturales y Gestión Ambiental
- Sistemas de Información Geográfica
- Estudio y Gestión del Agua
- Estudio y Gestión de Riesgos (Universidad Politécnica Salesiana, 2011-2014)

CIVABI (Centro de Investigación y Valorización de la Biodiversidad)

El centro de investigación se encarga de los recursos naturales renovables, para lograr un uso sostenible con la tecnología, uno de sus objetivos es promover trabajos de investigación en el campo de los productos naturales. En efecto sus líneas de investigación se mencionan a continuación:

- Química Analítica y Ambiental
- Microbiología
- Productos Naturales
- Botánica y Biodiversidad
- Biotecnología (Universidad Politécnica Salesiana, 2011-2014)

Los principales servicios de red que demandan estos centros de investigación para acceder a las comunicaciones en cualquier parte del mundo con una mejor calidad y de manera simultánea brindando además un uso compartido de recursos a través de la red estos servicios son tanto VOIP como Video Conferencia.

VOIP

Es la transmisión de voz sobre una red de datos que se encuentran basados en el estándar IP, empleando protocolos que corren en tiempo real, tanto el transmisor como el receptor están sincronizados para transmitir bilateralmente paquetes de voz en una misma transmisión es decir de manera simultánea. Cuenta con un cluster Cisco CallManager de la serie 7825 I3 versión 6.0, con capacidad de 300 end points

donde se encuentra el 60% empleado brindando el servicio IVR. (Universidad Politécnica Salesiana, 2011-2014)

Video Conferencia

Es un servicio de interacción visual, auditiva y verbal sobre protocolos IP en tiempo real, para este caso la comunicación entre los investigadores en cualquier parte del mundo, así es que ayuda a las comunicaciones presenciales para realizar un trabajo de investigación coordinado.

3.2.1 Aplicaciones de Internet 2

El desarrollo de las aplicaciones para las redes avanzadas se encuentra basado en la computación distribuida o conocida también como Grid, de este modo los investigadores pueden acceder a la información, a datos o a los recursos sin importar el lugar geográfico donde se encuentran para lograr así realizar un trabajo con sensación de presencia.

Actualmente en la UPS se están desarrollando proyectos bajo el cargo del Ing. Washigton Ramírez Msc. para redes avanzadas, no obstante la falta de seguridad hace que estos prototipos o demos no sean aplicados.

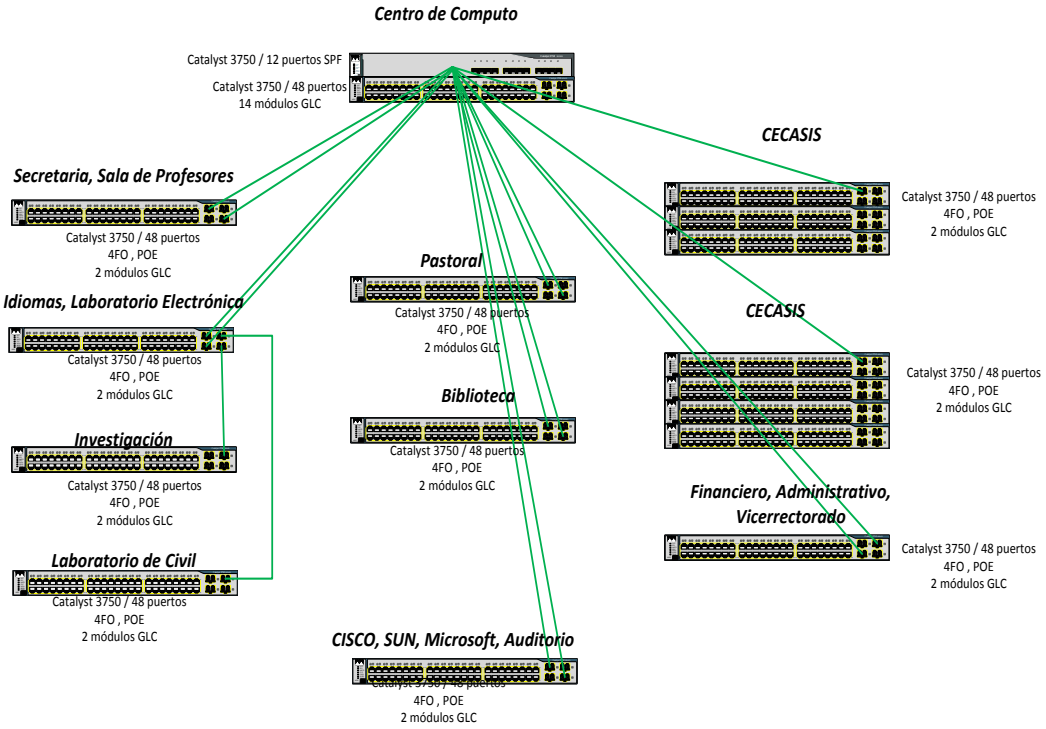
Principalmente están enfocados en el desarrollo de: Video Conferencia mediante el uso de multicast y la implementación de Clusters, dicho de otro modo es un conjunto de computadoras interconectas cuyo objetivo es trabajar en conjunto mediante la distribución de tareas es así que en este proyecto se emplea programación en paralelo.

Independientemente de los centros de investigación, adicionalmente se está manejando como línea de investigación la Telemedicina, en el área de Telepediatría, este proyecto se encuentra asociado con el Centro de Salud N°3 La Tola en la Ciudad de Quito, apoyado en el servicio de videoconferencia sin embargo no se encuentra en marcha.

3.2.2 Topología Actual de la Red UPS, Campus Sur

En la Universidad Politécnica Salesiana Sede Quito Campus Sur, la ubicación del Data Center es en el quinto piso del bloque principal en el Centro de Cómputo de la UPS; este como sitio principal alberga a: los servidores, el servicio de internet, los servicios para la red privada. Además cuenta con switches de distribución para cada área de la UPS tanto de manera geográfica como administrativa para los siete bloques que conforman la institución; para acceder a los servicios que esta ofrece, cuenta con switches de distribución de la serie Catalyst 3750 POE-48 conjuntamente con la serie Catalyst 2960 POE-48, y para el acceso a la red inalámbrica posee siete Access Point tanto de la serie Cisco 1310 GAK-9 como Cisco 1250, de hecho para tener una mejor administración y gestión de las antenas para el acceso inalámbrico emplea un Wlan Controller de la serie 2500. En la Figura 4 se muestra la distribución de los switches en el campus sur de la UPS Sede Quito.

Figura 4 Diagrama de la Topología de la UPS, Sede Quito Campus Sur



Fuente: Universidad Politécnica Salesiana

Modelo Jerárquico

Este modelo de arquitectura es útil para administrar la red y mejorar la disponibilidad de la red, debido a que su modelo separa la red en módulos o capas, cumpliendo con una función específica.

CISCO indica que los beneficios que se tiene al emplear el modelo jerárquico son los que se menciona a continuación:

- Costo
- Facilidad de compresión
- Crecimiento de la red modular
- Mejora el aislamiento de fallos
- Facilita los cambios en la infraestructura de la red

Este modelo está compuesto por tres capas que son: Core, Distribución y de Acceso.

Core

Esta capa del modelo provee un transporte rápido entre los switches de distribución ya que es la troncal de la red, cuyas funciones son:

- Trasporte rápido
- Alta fiabilidad
- Redundancia
- Tolerancia a fallos
- Baja latencia y buena capacidad de gestión (Bruno & Jordan, 2011, págs. 41-42)

Distribución

La función que desempeña es proporcionar conectividad basada en políticas de seguridad, además proporciona adición de rutas que se emplea como un resumen de rutas para el núcleo, por ello se ocupa de las siguientes funciones:

- Redundancia y Balanceo de Carga
- QoS
- Filtrado de Seguridad
- Acceso al grupo de trabajo
- Broadcast o Multicast
- Enrutamiento intervlan’s (Bruno & Jordan, 2011, pág. 42)

Acceso

Provee al usuario segmentos de la red local, brindando accesibilidad a los grupos de trabajo de la red con diferentes características como el ancho de banda, acceso a aplicaciones entre otras cuyas funciones son:

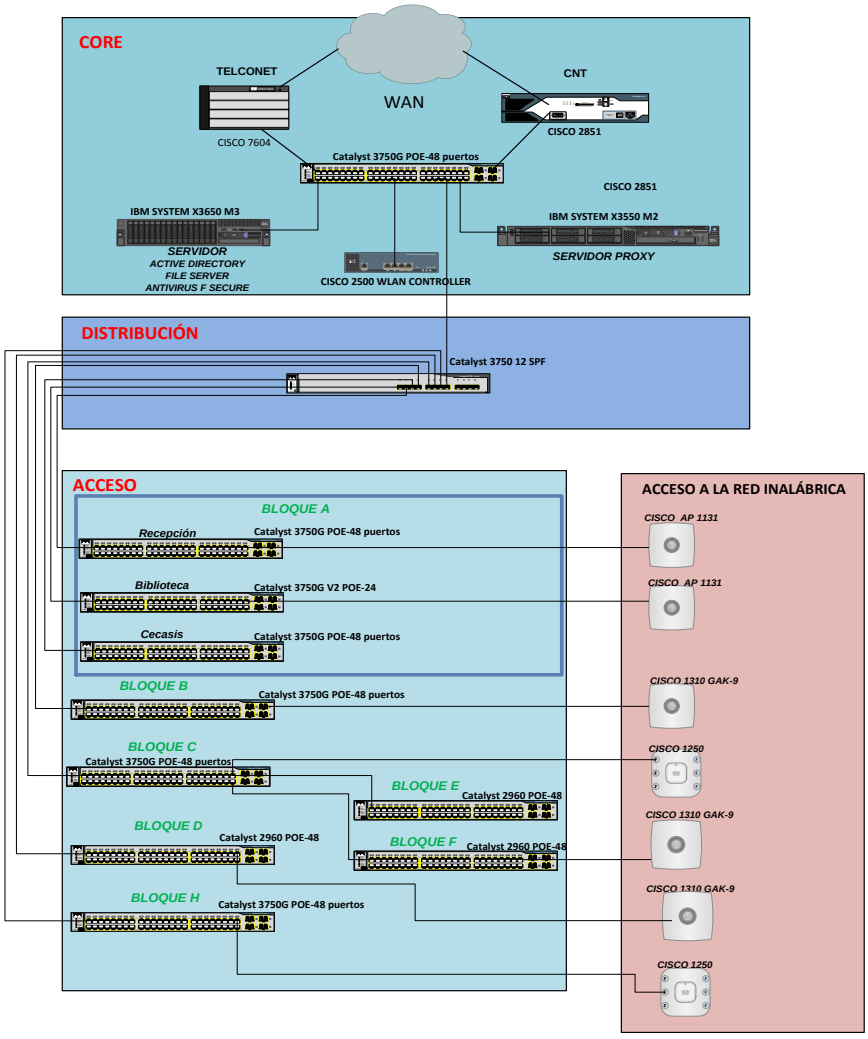
- Alta disponibilidad
- Puertos de seguridad
- Supresión de Broadcast
- QoS
- Limitación de velocidad
- Lista de control de acceso virtual
- Árbol de expansión
- Vlan auxiliar de VOIP (Bruno & Jordan, 2011, pág. 43)

Por consiguiente la UPS Sede Quito, Campus Sur proporciona un enlace redundante ISP para el servicio de internet y datos, cuenta con dos proveedores uno hacia CNT mediante un router CISCO 2851 y hacia TELCONET a través de un router CISCO 7604, sin embargo no proporciona redundancia para el enlace local. Esta capa de core está compuesto como núcleo por un switch Catalyst 3750G POE de 48 puertos donde están conectados dos servidores: un servidor proxy de la serie IBM SYSTEM X3550 M2 y un servidor que contiene Active Directory, File Server, Antivirus Fsecure de la serie IBM SYSTEM X3550 M3, además se encuentra conectado WAN CONTROLLER de la serie CISCO 2500 para proporcionar una mejor administración y gestión para el acceso a las redes inalámbricas.

En la capa de distribución cuenta con un switch Catalyst 3750 12; aquí se encuentran las políticas de conectividad, pero no cuenta con redundancia debido a que solo hay un switch de distribución.

Finalmente está la capa de acceso que cuenta con seis switch Catalyst 3750 POE 48 de puertos, y dos switch Catalyst 2960 POE de 48 puertos donde están conectadas Access Points tanto de la serie CISCO 1310 GAK-9 como la serie CISCO 1250 para proveer conexión inalámbrica. El modelo jerárquico de la red de la UPS se muestra en la figura 5.

Figura 5 Modelo Jerárquico de la Red de la UPS Sede Quito Campus Sur



Fuente: Universidad Politécnica Salesiana
Elaborado por: Berenice Arguero

3.3 IP versión 6

IPv6 es un protocolo de internet de nueva generación, surgió en el año de 1995, pero se estableció definitivamente sus características y especificaciones en el RFC 2460 en diciembre del 1998; debido a que el espacio de las direcciones de IPv4 se están agotando precipitadamente especialmente en Asia, se buscó una solución, óptima, el cual fue crear un nuevo protocolo de internet, gracias a los creadores Steven Deering y Robert Hiden, y que actualmente ya está en uso.

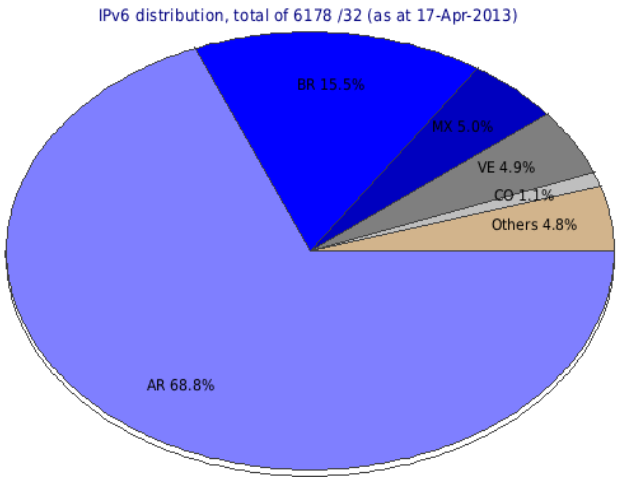
IPv4 ha sobrevivió gracias a los diferentes mecanismos como NAT (Network Address Traslation), CIDR (Classless Interdomain Routing), también DHCP (Dynamic Host Control Protocol), PPP (Point to Point Protocol) los cuales solventan en parte la falta de direcciones. A partir del 2000 comienza la implementación de IPv6 en las plataformas de red, brindando servicios y aplicaciones mejoradas que son transparente para el usuario, puesto que aún no se habla de eliminación de IPv4 sino de coexistencia de estos dos protocolos en internet.

Existen proyectos ya desarrollados de IPv6 para las redes de educación e investigación relacionados directamente con el Internet 2, por ejemplo se puede mencionar el proyecto desarrollado en Europa en el año 2004 conocido como 6NET y Euro6IX que implementaron del protocolo IPv6 a la red GÉANT, logrando cumplir el objetivo propuesto, la interconexión de las redes de educación e investigación con las redes nacionales con resultados óptimos; este proyecto dio la pauta para ahora contar con una interconexión intercontinental con cada una de las redes académicas.

El acogimiento de IPv6 en Latinoamérica ha sido de gran importancia, no solo por el agotamiento de direcciones de IPv4 sino por la gran capacidad de direccionamiento IPv6 ya que se habla de 2^{128} direcciones, por lo que ya no se tiene la necesidad de realizar CIDR , NAT debido al espacio de direccionamiento; además de un manejo mejorado de los paquetes por la reducción de campos en el formato de cabecera IPv6 logrando así mejorar las características de calidad de servicio QoS, clase de servicio, denominada como CoS, además de la seguridad integrada. Por tal razón la adopción

de IPv6 según los datos proporcionados por la LACNIC en Latinoamérica indica un incremento en los últimos años como se muestra en la figura 6.

Figura 6 Diagrama de Pastel de Distribución de Direcciones IPv6 en número de /32, ya asignadas por LACNIC entre los países de la región.



Fuente: LACNIC

Ecuador tiene asignado un 2.1% de redes IPv6 /32 del espacio de direcciones para Latinoamérica en el último periodo según los datos registrados por la LACNIC. A la red CEDIA se le asignó la dirección 2800:68:: /32 y a su vez se ha dividido en redes de /48 para las Universidades y Centros de Investigación. En el Reto IPv6 CEDIA 2011 se puede verificar la asignación de la dirección 2800:68:0016::/48 para la Universidad Politécnica Salesiana.

En el año 2010 la red CEDIA menciona que eliminó los túneles de IPv6 sobre IPv4 por lo que, se implantó en el core nacional IPv6 nativo, brindando los servicios: Web, Mail, DNS, NTP, XMPP, IPv6 multicast, redes de laboratorio IPv6, a una alta velocidad con un nivel bajo de congestión.

3.3.1 Arquitectura del Protocolo IPv6

La arquitectura de IPv6, con respecto al protocolo IPv4 posee características mejoradas como son: un rápido procesamiento de los paquetes, debido a la disminución del tamaño de la cabecera, sin embargo tiene mayor flexibilidad para extender la cabecera con campos adicionales, dando así la posibilidad que la carga

útil del paquete sea más de 65.535 bytes (6SOS, 2004). Uno de los usos de las cabeceras de extensión es la movilidad, por ello hace uso de dichas cabeceras para tener la capacidad de mantener una misma dirección IP aunque se desplace físicamente a otra red.

Además tiene la funcionalidad de autoconfiguración de las direcciones en los dispositivos finales; si no se tiene un servidor de DHCPv6, la dirección IP es proporcionada tanto por el router que da el prefijo de la red asociada y por el identificador de interfaz, caso contrario con el servidor de DCHPv6 envía los parámetros de red al host.

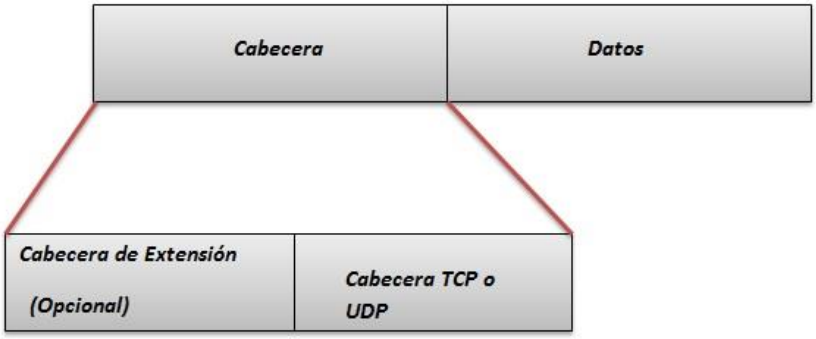
Una ventaja sobre de IPv4, son los campos que se encuentra en la cabecera IPV6; el campo de clase de tráfico provee la calidad de servicio, es decir da el tratamiento o la manipulación del paquete para poder diferenciar la prioridad del paquete o el tipo de servicio, y el otro campo es el etiquetado de flujo, que otorga la clase de servicio, brindando la facilidad de distinguir el tipo de tráfico y dar un tratamiento especial, más aún si se trabaja con servicios en tiempo real.

Como una característica adicional mejorada es la seguridad, dado que proporciona seguridad de tráfico con autenticación, seguridad de carga encapsulada, adicionalmente en IPv6 ya viene de manera intrínseca el protocolo de seguridad IPSec.

3.3.1.1 Paquete IPv6

El paquete IPv6 está formado por dos campos: cabecera que a su vez incluye las cabeceras de extensión que son opcionales, y la cabecera TCP o UDP, los datos que no superan los 64 Kb, las especificaciones y características está dado por la RFC 2460. En la figura 7 se puede observar el formato del paquete IPv6.

Figura 7 Formato del Paquete IPv6



Fuente: (Yángüez, 2012)

3.3.1.1.1 Formato de la Cabecera IPv6

La cabecera del protocolo de internet IPv6 fue desarrollada a base del formato de cabecera IPv4, con un tamaño de 40 bytes, como consecuencia de la eliminación de algunos campos dentro de la cabecera, esta reducción en el formato de la cabecera provoca que la convergencia del paquete sea más rápida y con un reenvío más eficiente. El formato de la cabecera es sencillo, está formada por seis campos de opciones y dos campos de direcciones como se puede apreciar en la figura 8, esta información es proporcionada por la RFC 2460, que indica la información de cada uno de los campos de la cabecera IPv6.

Figura 8 Formato de la Cabecera IPv6

Fuente: RFC 2460

Versión (Version): El valor del tamaño de campo es de 4 bits e indica la versión del protocolo de internet.

Clase de Tráfico (Traffic Class): Está formado por 8 bits, con un valor por defecto de cero; este campo es empleado para identificar y distinguir el tipo de prioridad del paquete IPv6.

Etiqueta de Flujo (Flow Label): El tamaño del campo es de 20 bits, da la opción de brindar un procedimiento especial a los paquetes IPv6, donde se habla de la calidad de servicio. Este campo no tiene un valor por defecto, pero se pone en cero sí el host, o un enrutador no tiene la capacidad de soportar el etiquetado de flujo.

Longitud de la Carga Útil (Payload Length): El tamaño del campo es de 16 bits, son los contenidos incluyendo las extensiones que vienen después de la cabecera IPv6, tiene dos funciones: identificar que tipo de extensión se incluirá después de la cabecera, además identifica los protocolos de capa superior.

Cabecera Siguiente (Next Header): El tamaño del campo es de 8 bits, el cual identifica el tipo de cabecera de extensión que sigue inmediatamente a la cabecera IPv6.

Límites de Salto (Hop Limit): El tamaño del campo es de 8 bits, este indica el tiempo de vida del paquete IPv6; por cada nodo que se reenvía el paquete este valor se resta uno, si llega a un valor de cero el paquete es descartado, esto evita generar lazos de enrutamiento.

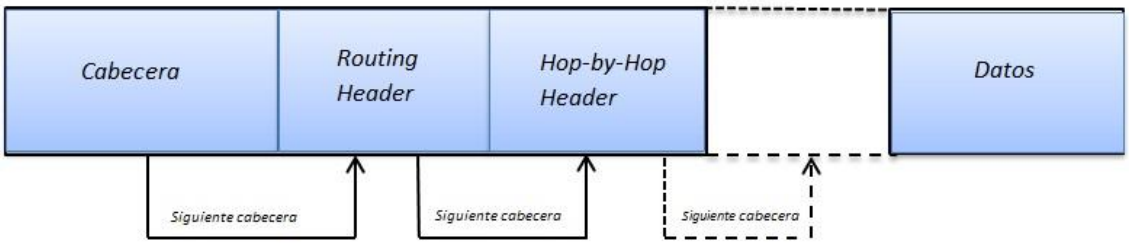
Dirección Origen (Source Address : El tamaño del campo es de 128 bits, que representa la dirección IP donde se origina el paquete.

Dirección Destino (Destination Address): El tamaño del campo es de 128 bits, este representa la dirección IP hacia donde se quiere llegar con el paquete.

3.3.1.1.2 Formato de la Cabecera de Extensión IPv6

Los autores Juan Alberto Lahera y Carlos Gonzáles indican que las cabeceras de extensión ofrecen servicios y mejoras comparando con el modelo interior, ya que en IPv6 se ha eliminado información de cabecera principal, en cambio se aumentaron cabeceras adicionales que son opcionales, las cuales son: Hop.by.hop, Routing, Fragment, Destination Option Header entre otros; se puede apreciar el formato de la cabecera de extensión en la figura 9(diapositiva 24)

Figura 9 Formato de la Cabecera de Extensión IPv6



Fuente: (Yángüez, 2012, pág. 27)

Las cabeceras de extensión se encuentran definidas por el campo de siguiente cabecera (next header) que sigue inmediatamente de la cabecera IPv6, cuya función es incorporar información adicional al paquete si es necesario; estos campos son examinados en orden de aparición en los nodos de los destinos finales.

En la tabla 1 se indica el valores que identifican a la cabecera de extensión y del protocolo que se coloca en el campo siguiente cabecera. Estos valores son asignados por la IANA, además las especificaciones están dadas por la RFC 2460.

Tabla 1 Valor asignado para la Cabecera de Extensión

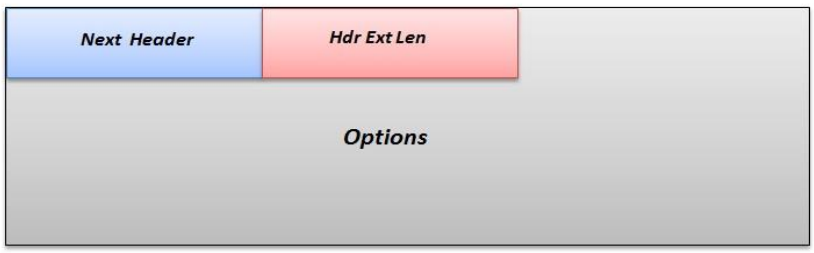
Valor	Cabeceras de Extensión
0	Hop.by.hop option
43	Routing
44	Fragment
50	Encapsulating Security Payload (ESP)
51	Authentication Header (AH)
59	No next header
60	Destination Option
62	Mobility Header
Valor	**Protocolos**
6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
58	ICMP

Fuente: (The 6NET, Consortium, 2005, pág. 10)

Hop-by-Hop

Es una de las cabeceras de extensión, identificada por el valor de cero en el campo Next Header de la cabecera IPv6, cuya finalidad es llevar información adicional dentro del paquete IPv6, que será identificado por cada nodo que se encuentra hasta llegar a su destino. Esta cabecera extra está formada por tres campos que se detallan a continuación.

Figura 10 Cabecera de Extensión Hop-by-Hop



Fuente: RFC 2460

Next Header, el tamaño de este campo es de 8 bits, identifica el tipo de cabecera que se anexara después de la cabecera Hop-by-hop.

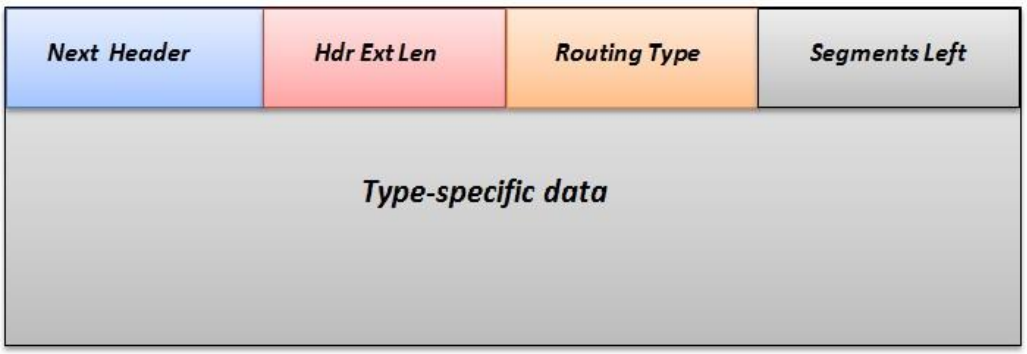
Hdr Ext Len, el tamaño de este campo es de 8 bits, indica la longitud de la cabecera formado por ocho octetos, excluyendo el primero.

Options, su longitud es variable formado por 8 octetos, contiene uno o varios TLV –econded, estas opciones son: Option Type, Opt Data Len, Option Data con el formato correspondiente.

Routing Header

Esta cabecera de extensión es utilizada con la finalidad de especificar los nodos intermedios por donde va a pasar el paquete, esta función es equivalente a IPv4 a Loose Source y Record Route Option, con el siguiente formato que se puede observar en el figura 11.

Figura 11 Cabecera de Extensión Routing Header



Fuente: RFC 2460

Next Header, este campo tiene un tamaño de 8 bits cuya función es identificar el tipo de cabecera que va después de la cabecera de enrutamiento.

Hdr Ext Len, el tamaño de campo es de 8 bits, e indica la longitud de la cabecera de enrutamiento formado por ocho octetos, excluyendo el primero.

Routing Type, está conformado por 8 bits, este campo identifica el tipo o clase de una cabecera de enrutamiento en particular.

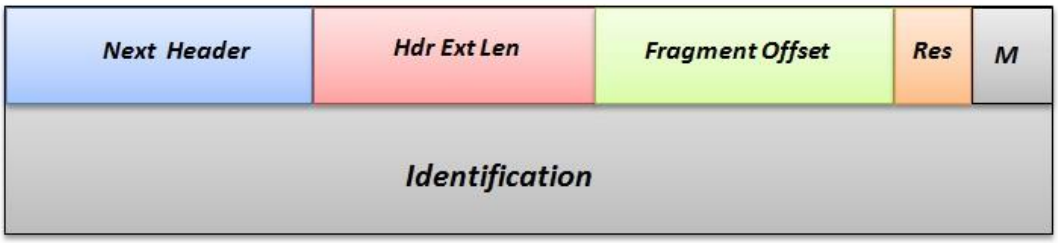
Segments Left, formado por 8 bits indica el número de nodos intermedios que se tiene que atravesar antes de llegar el destino final.

Type-specific data, el tamaño del campo está formado por 8 octetos de largo, es decir es de longitud variable, quien determina el tipo de datos está dado por el campo Routing Type.

Fragment Header

Está identificada por el valor de 44 en la campo Next Header de la cabecera IPv6, con el propósito de poder enviar un paquete con un tamaño mayor de lo limitado por la MTU desde el origen hasta el destino. En la figura 12 se detalla el formato de esta cabecera de extensión.

Figura 12 Cabecera de Extensión Fragment Header



Fuente: RFC 2460

Next Header: el tamaño de este campo es de 8 bits, identifica el tipo de cabecera que va inmediatamente después de la cabecera de fragmentación.

Reserved:el tamaño del campo es de 8 bits, solo para la trasmisión este campo se encuentra inicializado con un valor de cero.

Fragment Offset el tamaño del campo es de 13 bits, cuya función es controlar el proceso de fragmentación.

Res: el tamaño del campo es de 2 bits, se emplea solo para la recepción y se encuentra inicializado con un valor de cero.

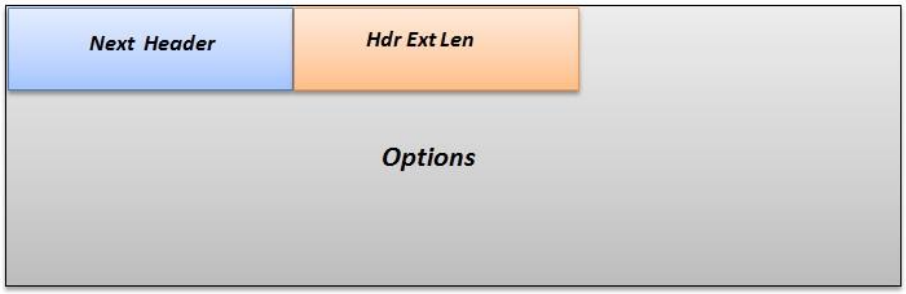
Mflag: este campo permite indicar colocando con un valor de 1 si habrá más fragmentos y con un valor de cero si es el último fragmento.

Identification: está formado por 32 bits, cuyo propósito es volver a armar en paquete en el destino, este valor es diferente para cada paquete fragmentado dado por el origen.

Destination Option Header

Está identificada por el valor 60 en el campo Next Header de la cabecera IPv6, cuya objetivo es llevar información adicional, que será analizada por el destino. Constituido por tres campos, con el siguiente formato que se puede apreciar en la figura 13.

Figura 13 Cabecera de Extensión Destination Option Header



Fuente: RFC 2460

Next Header, el tamaño de este campo es de 8 bits, identifica el tipo de cabecera que se anexara después de la cabecera Destination Option.

Hdr Ext Len, el tamaño de este campo es de 8 bits, indica la longitud de la cabecera formado por ocho octetos, excluyendo el primero.

Options , su longitud es variable formado por ocho octetos, contiene uno o varios TLV –econded, estas opciones son : Option Type, Opt Data Len, Option Data con el formato correspondiente.

3.3.1.2 Direccionamiento IPv6

La dirección IP del protocolo de internet IPv6 está formada por 128 bits, representada por 8 campos hexadecimales de 16 bits o cuatro dígitos separados por dos puntos, establecido por la RFC 4291, como se observar a continuación.

Figura 14 Ejemplo de dirección IPv6

Fuente: (Castro, 2011, pág. 12)

3.3.1.2.1 Formato y Representación del Paquete IPv6

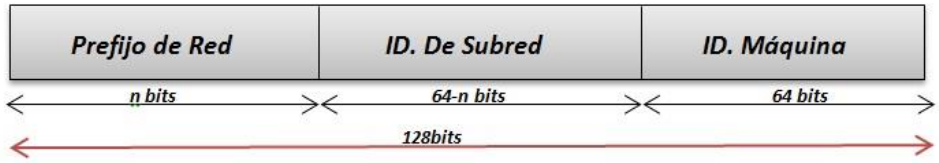
Las direcciones IPv6 están formadas por 3 campos principales que son: el prefijo global, el identificador de la subred y el identificador de interfaz, el formato del paquete IPv6 se representa en la figura 15.

Prefijo Global, es el conjunto de direcciones que se asignan a una organización.

Identificador de Subred, como su nombre indica, este campo permite identificar a la subred dentro de la red de área local.

Identificador de Interfaz, realiza la identificación de la interfaz del host dentro de la subred.

Figura 15 Formato y representación del paquete IPv6



Fuente: (Castro, 2011, pág. 12)

En una dirección IPv6 no es necesario escribir los ceros que se encuentran a la izquierda de un campo determinado, además las cadenas de ceros se puede suprimir y remplazarlos por con dos puntos seguidos, esta regla es aplicada una sola vez en una misma dirección, por ejemplo:

cbba:0000:0000:feb21:7678:0db6:45d1

cbba::feb21:7678:0db6:45d1

3.3.1.2.2 Tipo de Direcciones IPv6

Unicast

Este tipo de direcciones identifican a una sola interfaz de la red, y se encuentra dividida en:

- Unicast de enlace que son usadas para la autoconfiguración, descubrimiento de vecinos y trabajo sin los enrutadores. (CEDIA, 2010, pág. 22)
- Unicast privadas, como su nombre lo indica son usadas en un ambiente de red local y son independientes a las direcciones que entrega el ISP.

Multicast

Al contrario de las unicast este identifica a un conjunto de interfaces de diferentes nodos de la red, los paquetes enviados a las interfaces son todos a la vez, se emplea para aplicaciones de transmisión múltiple.

Anycast

Se usan para un identificar a un grupo de interfaces en diferentes nodos de red, pero a diferencia de las multicast los paquetes son enviados uno a la vez a cualquiera de las interfaces la más cercana.

Lazo Local

Estas direcciones no se emplean para realizar enrutamiento, sino únicamente para establecer conectividad entre los enlaces locales.

FECx :xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

FEDx :xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

FEEx :xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

FEFx: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

Loopback

Es una interfaz que no existe físicamente, es decir es virtual pero cumple la misma funcionalidad de una interfaz real pero los paquetes no salen de la máquina y está representada por la siguiente dirección IPv6:

0000:0000:0000:0000:0000:0000:0001

::1

En la tabla 2 se indica las direcciones que se encuentran restringidas o de uso privado como:

Tabla 2 Direcciones IPv6 restringidas o de uso privado

Notación IPv6	Prefijo Binario	Tipo de Dirección
0::0 /128	0000….0 (128 bits)	Dirección sin Especificar
0::1 /128	0000….1 (128 bits)	Dirección de Loopback
FC00:: / 7	1111 110…….	Unique Local Unicast (RFC 4193)
FE80:: / 10	1111 1110 10…….	Link Local Unicast (RFC 4291)
FF00:: / 8	1111 1111	Multicast (RFC 4291)
2000:: / 3	001….	Prefijo asignado por la IANA
2001:DB8::/ 32		RFC 3849

Fuente: (Castro, 2011, pág. 13)

3.3.2 Vulnerabilidades de IPv6

El hablar de vulnerabilidades identifica cuáles son los riesgos a los que se expone Internet 2 para que de una u otra manera estar preparados para cualquier eventualidad, a su vez, la red académica avanzada hace uso único de IPv6 está expuesta a las vulnerabilidades que esta posee.

Uno de los puntos que afectan la seguridad de la red en entorno IPv6 son las cabeceras de extensión, debido a que un atacante puede llegar a manipular este tipo de cabeceras para realizar un ataque. Esta manipulación puede hacer que los paquetes tengan un gran número de cabeceras de extensión y por consiguiente su carga útil será mayor, provocando probablemente que el paquete no sea revisado por un firewall, el cual desempeña las funciones de análisis a las cabeceras de extensión, en vista de que este se fragmenta, por lo tanto, para este tipo de ataques a la red, una

solución sería realizar un filtrado de las cabeceras de extensión especialmente de las cabeceras: Destination Option, Mobility, Routing Header.

Asimismo se menciona el uso ICMPv6 ya que este cumple un papel importante en IPv6 puesto que ayuda a verificar la conectividad de extremo a extremo a través del empleo del ping y el traceroute; sin embargo este es un punto de riesgo debido a que este recurso proporciona un método para realizar un ataque a la infraestructura de la red especialmente en el consumo de recursos, ya que el atacante podría generar múltiples paquetes ICMPv6 para alcanzar al firewall logrando así causar un alto consumo en la red en vista de que un router o un firewall descartan el paquete cuando el límite de salto es igual a uno, enviando como respuesta enviando un ICMPv6 de tiempo extendido al origen del paquete generando así un bucle infinito; con este comportamiento el atacante puede inundar de paquetes ICMPv6 para alcanzar al firewall ya que el límite de salto se reduce a cero, causando un ataque al consumo de la red.

Los únicos mensajes que se propagan en una red LAN son aquellos que tengan como límite de salto el valor establecido de 255, es así que un dispositivo de capa 3 debe descartar un paquete cuyo límite de saltos sea menor a 255; una de las soluciones es bloquear todos los tipos de mensajes ICMPv6 que no han sido asignados por la IANA y adicionalmente bloquear los paquetes ICMPv6 que provengan de una red externa.

En último término se menciona como un punto desfavorable en IPv6, el empleo de multicast, por la razón que este es un mecanismo de difusión empleado para: el descubrimiento de vecinos, configuración dinámica de direcciones y aplicaciones multimedia, de ahí que el atacante hace uso de este para enviar tráfico a direcciones multicast, y cada dispositivo de la red responde cada petición el atacante obtiene información acerca de la red, esto se debe a que en IPv6 no existe la fase de reconocimiento y el dispositivo entrega su información. Frente a este tipo de ataque se debe realizar la comprobación de la dirección de origen de los paquetes en lugar de inspeccionar la dirección de destino, de manera que se negaría cualquier paquete que

utilice una dirección multicast como dirección origen. (Bruno & Jordan, 2011, págs. 22-23)

3.4 Protocolo de Seguridad IPSec

La seguridad es un punto destacado en los requerimientos de la red que va a depender de las aplicaciones que trabajan en el entorno de la red, motivo por el cual el brindar seguridad a nivel de capa de red garantiza que el tráfico procesado por los protocolos de niveles superiores se transmitan de manera segura, protegida y de una manera transparente para el usuario. Una de las maneras más eficientes de lograr este cometido es mediante el uso de IPSec, el mismo que usa la gestión de intercambio de claves compartidas para cifrar y autenticar el origen de los datos.

En IPv6 se incluye implícitamente el protocolo de seguridad IPSec, debido a su arquitectura extensible con la posibilidad de usar o no los mecanismos de cifrado y de autenticación de IPSec.

Este protocolo fue desarrollado por el Grupo de Seguridad de la IETF (Internet Engineering Task Force), con la finalidad de desarrollar mecanismos de protección al protocolo IP, y así brindar seguridad a nivel de la capa de red, proporcionando servicios de seguridad criptográfica para lograr soportar autenticación, integridad, control de acceso y confidencialidad.

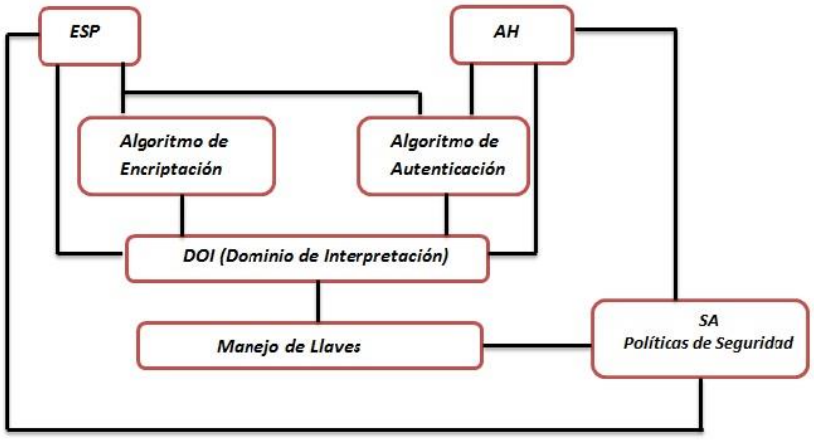
Este conjunto de protocolos de seguridad interoperable de alta calidad, presta servicios como la encriptación, que son técnicas matemáticas para codificar la información con el fin de proteger la misma, este se emplea tanto en el control de acceso como para la confidencialidad. Como otro servicio importante es la capacidad de que la información enviada no sea manipulada o cambiada y se conoce como la integridad de la información, este es un servicio no orientado a conexión.

3.4.1 Arquitectura de IPSec

IPSec provee servicios de autenticación y encriptación para Internet, protegiendo los datos a nivel de capa red, para lo cual cuenta con protocolos para este fin, como son el protocolo de Autenticación AH y el protocolo de Carga de Seguridad Encapsulada ESP, además de un protocolo para el manejo de llaves.

Su finalidad es establecer canales seguros o IPSec Domain of Interpretation conocido por las siglas DOI, mediante la negociación de parámetros de seguridad que previamente ya se estableció en las asociaciones de seguridad. La esquematización de la arquitectura IPSec se puede observar en la figura 16.

Figura 16 Arquitectura de IPSec



Fuente: (Mendoza & Carlos, 2002, pág. 4)

3.4.1.1 Modos de Funcionamiento

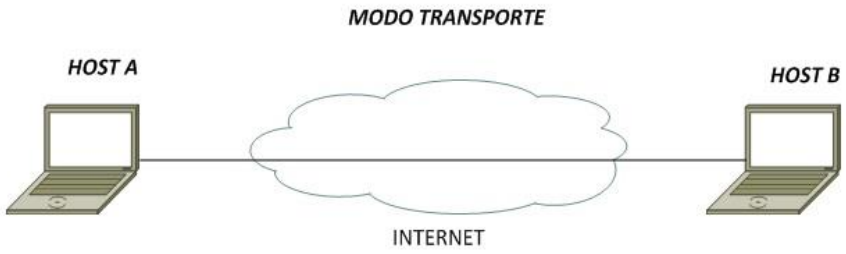
El protocolo IPSec posee dos modos de funcionamiento, el modo transporte y el modo túnel, su empleo depende de la infraestructura que se desea brindar autenticación y encriptación de la información.

- **Modo Transporte**

Este modo de funcionamiento es empleado para proteger la comunicación de extremo a extremo, es decir la autenticación y la encriptación se encuentran a nivel de host;

esto requiere que los dos extremos de la comunicación conozcan el protocolo IPSec. En la figura 17 se muestra el funcionamiento de IPSec en modo transporte.

Figura 17 Funcionamiento de IPSec en Modo Transporte

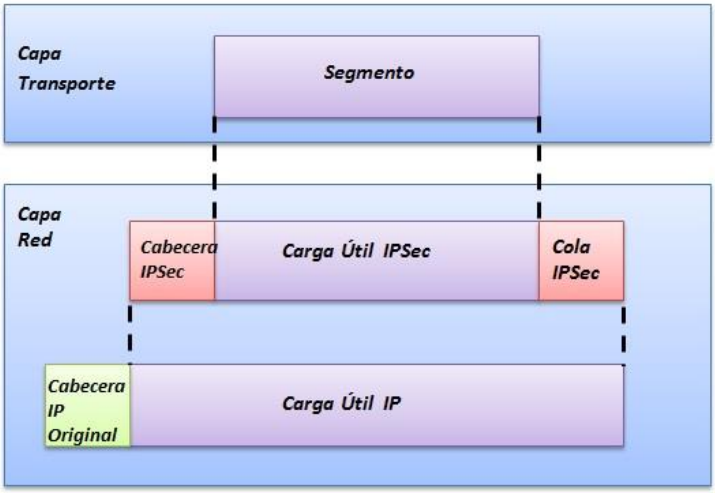


Fuente: RFC 2401

Tanto el protocolo AH como ESP pueden ser empleados en el modo transporte, pero cuando se utilicen estos dos protocolos, primero se debe aplicar la cabecera ESP y después la cabecera AH con el fin que la integridad de los datos sea aplicada a la carga útil de ESP.

La cabecera y la cola de los protocolos de IPSec, son aplicadas a la carga útil de la capa de red que proviene de los niveles superiores los cuales se requieren proteger; además se encuentra ubicado a continuación de la cabecera IP original, es visible pero no es modificado ni cifrado. En el figura 18 se puede determinar el la ubicación de los protocolos de autenticación.

Figura 18 Formato de la cabecera en modo transporte de los protocolos IPSec

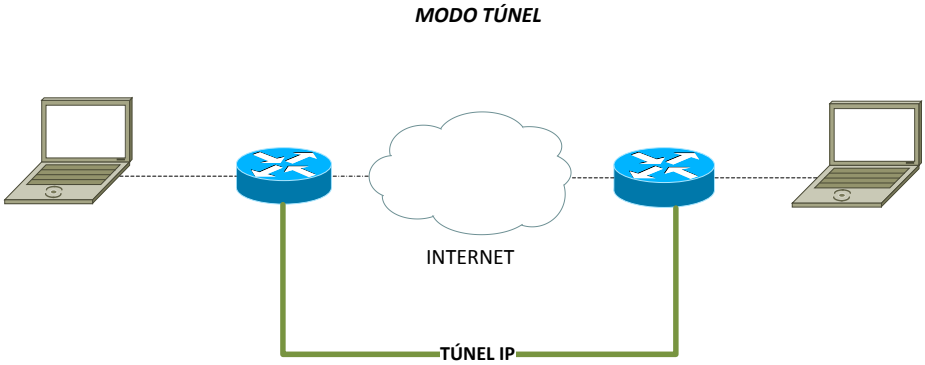


Fuente: (Yángüez, 2012, pág. 51)

- **Modo Túnel**

Este es implementado a: routes de acceso a internet, a routers vecinos a los nodos finales, a firewalls o a un host a lo que se denomina gateways IPSec cuya función es centralizar el tráfico en un solo equipo mediante gateways IPSec el cual identifica la red a proteger bajo una misma dirección IP; al emplear el protocolo ESP en modo túnel este permite ocultar la identidad de los nodos que se están comunicando. En la figura 19 se muestra el funcionamiento de IPSec en modo túnel.

Figura 19 Funcionamiento de IPSec en Modo Túnel

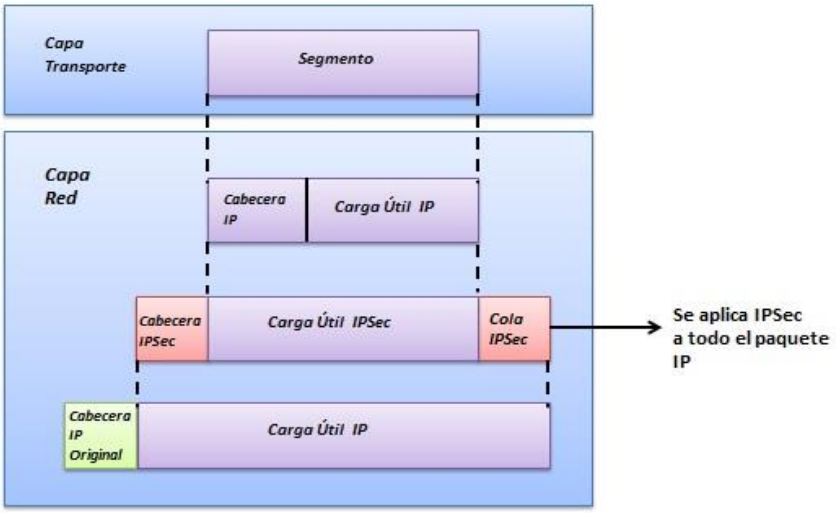


Fuente: RFC 2401

La autenticación y cifrado abarca a todo el paquete original, donde el paquete IP es encapsulado con la o las cabeceras de IPSec, añadiendo así un encabezado IP, el cual posee dos encabezados IP interior que es creado por el host y el exterior que es agregado por el dispositivo que brinda la seguridad.

La cabecera y la cola de los protocolos AH como el protocolo ESP se aplica a la carga útil de la capa de red, el cual proviene de los niveles superiores y son los datos que se quiere proteger y después se añade una nueva cabecera IP tipo túnel, el cual no es autenticado ni cifrado. La ubicación de los protocolos de IPSec se puede observar en la figura 20.

Figura 20 Formato de la cabecera en modo túnel de los protocolos IPSec



Fuente: (Yángüez, 2012, pág. 53)

En la tabla 3 se puede apreciar las ventajas y desventajas de los dos modos, uno al respecto del otro, lo cual depende el escenario donde se requiera emplear y que se desea proteger.

Tabla 3 Tabla comparativa entre los modos de funcionamiento de IPSec

Modo Transporte	**Modo Túnel**
La seguridad se emplea en una comunicación de extremo a extremo.	Su implementación es más sencilla debido a que permite incorporar la seguridad sin necesidad de incluir IPSec en los nodos finales extremo a extremo. (Yángüez, 2012, pág. 55)
En la encapsulación la cabecera original IP es visible.	Protege a la parte más expuesta del trayecto que es la infraestructura, pero hay menor seguridad en la red.
La información que se protege es únicamente el protocolo TCP o UDP, como los datos de la capa aplicación. (Pérez, 2001, pág. 56)	La autenticación y cifrado se realiza a todo el paquete original

Elaborado por: Berenice Arguero

3.4.1.2 Asociaciones de Seguridad de IPSec

Al hablar de interoperabilidad, IPSec tiene cualidad de trabajar en cualquier plataforma o sistema de trabajo debido a su estructura modular, para lo cual IPSec opera mediante Asociaciones de Seguridad (SA), y que a su vez se encuentran almacenadas en una base de datos conocida como Base de Datos de Asociación de Seguridad (SADB) referida a la RFC 2401.

Las SA´s tienen el propósito de especificar las propiedades de la seguridad para el flujo de tráfico pero se da de manera unidireccional; como se requiere es proteger la integridad de los datos tanto de salida como de entrada, se necesita una SA para cada una de ellas y estas se caracterizan por los siguientes puntos: índice de parámetros de seguridad, dirección IP destino y el identificador del protocolo seguridad. En la figura 21 se indica el formato de las SA´s.

Figura 21 Formato de Asociación de Seguridad de IPSec

Fuente: (Alarcos & De la Hoz, 2006, pág. 24)

Los campos son:

1. Índice de parámetro de Seguridad SPI, es un valor arbitrario de 32 bits para identificar a una SA, el cual se trasmite en una de las cabeceras del protocolo de seguridad tanto AH como ESP, según se requieran.

2. Dirección IP destino, esta puede ser una dirección unicast o un grupo de direcciones multicast pero para la definición de las políticas se requiere direcciones unicast.

3. Identificador del protocolo de seguridad que puede ser AH como ESP.

Los servicios de seguridad que ofrece una SA, se encuentran albergados en una base de datos para la gestión de las SA´s para lo cual integra dos bases de datos:

a) SPD, Base de Datos de Políticas de Seguridad, es donde se especifican las políticas para determinar el tipo de tratamiento que se dará al tráfico tanto entrante como saliente.

b) SAD, Base de Datos de Asociaciones de Seguridad, esta contiene los parámetros requeridos para asociar una interfaz con cada una de las SA´s que se encuentran de manera activa.

3.4.1.3 Modos de Operación de SA

Tanto el protocolo AH y el protocolo ESP utilizan las SA's para realizar la seguridad de los datos y el protocolo IKE, su función principal es establecer y mantener de las SA´s, para lo cual existe dos modos de operación: en modo transporte que se emplea en un escenario entre dos host, cuya función va a depender de la seguridad que se va aplicar cuando se añade el protocolo ESP, este brinda seguridad solo a los protocolos de capas superiores, mientras que el protocolo AH protege a las partes seleccionadas de la cabecera IP y de la cabecera de extensión.

En modo túnel la SA se aplica a un túnel IP, este modo se aplica cuando se tiene escenarios donde: un extremo de la SA sea un Security Gateway, una SA entre dos Security Gateway, o una SA entre un host y un Security Gateway, donde hay la necesidad de evitar problemas con la fragmentación y re-ensamblaje de paquetes IPSec, y donde existan múltiples trayectorias. En este modo el protocolo AH protege todo el paquete tanto las partes de la cabecera IP y ESP solamente protege el paquete IP.

3.4.1.4 Combinaciones de SA

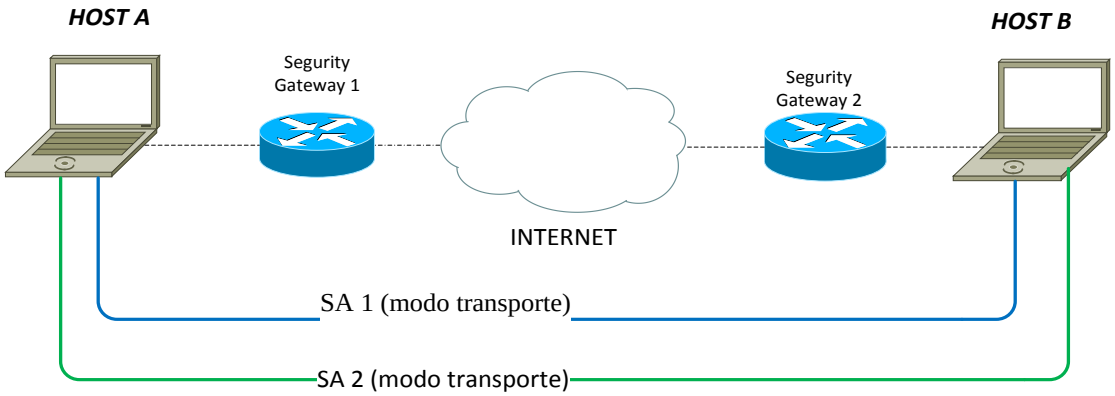
Este se aplica cuando una sola SA, no puede realizar varios servicios de seguridad debido a que solo permite aplicar un único protocolo IPSec ya sea AH o ESP para un flujo de tráfico específico, para lo cual demanda implementar varias SA's para lograr

cumplir la política de seguridad requerida teniendo como resultado dos tipos de combinaciones.

Transporte Adyacente

En el transporte adyacente se aplica más de un protocolo de seguridad IPSec, donde se puede combinar el protocolo AH y ESP sobre un mismo paquete IP, sin utilizar túneles IP permitiendo un nivel de combinación. En la Figura 22 se muestra la combinación de la SA en tipo transporte adyacente.

Figura 22 Combinación de SA's , tipo Transporte Adyacente



Fuente: RFC 2401

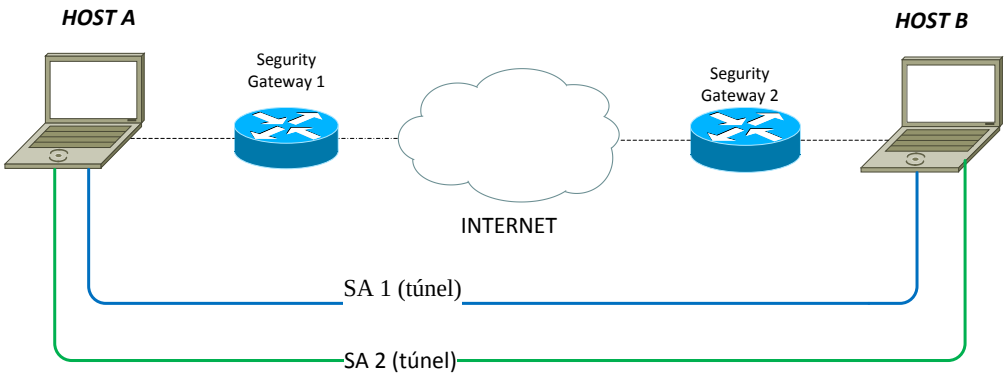
Entre Túneles

En esta combinación se aplican múltiples SA´s implementadas en múltiples túneles IP, donde existen tres casos de combinación.

Caso 1: Ambos extremos de las SA´s son las mismas

Se emplea dos asociaciones de seguridad donde se puede combinar los protocolos AH y ESP uno para emplear en el túnel interno y el otro para el túnel externo. La combinación de las SA´s se da en el entorno de dos host que se encuentran en los extremos. En la figura 23 se observa la comunicación entre ambos extremos donde las SA´s son las mismas.

Figura 23 Combinación Entre Túneles, Caso 1

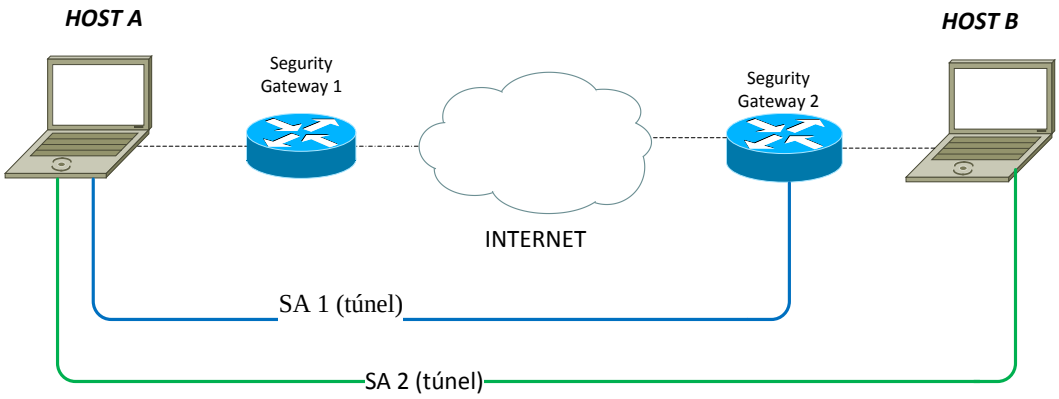


Fuente: RFC 2401

Caso 2: Un extremo de las SA's es igual

En este caso uno de los extremos de las SA's es el mismo y en el otro no, el túnel interno o externo puede aplicarse el protocolo como AH o el protocolo ESP. Una de las asociaciones de seguridad está entre un host1 y un Segurity Gateway 2 y la otra asociación de seguridad esta desde el host A y el host B. La combinación entre túneles, caso 2 se puede apreciar en la Figura 24.

Figura 24 Combinación Entre Túneles, Caso 2

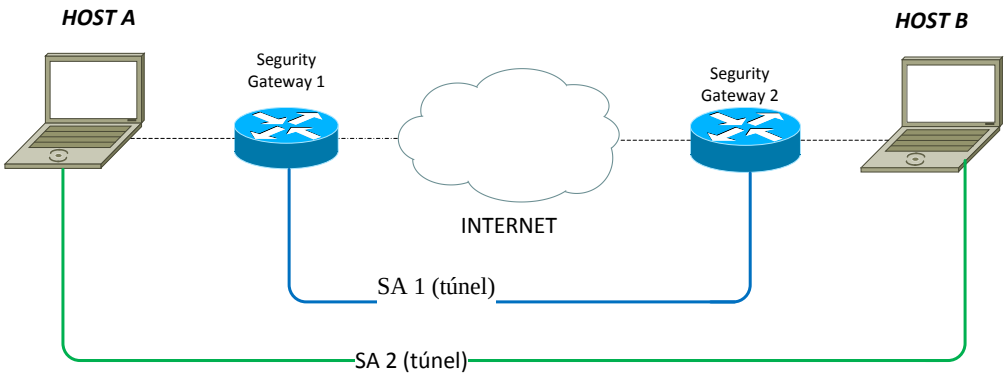


Fuente: RFC 2401

Caso 3: Ningún de los extremos es igual

En este tipo de escenarios, ninguno de los extremos las SA's son las mismas por lo que los túneles interno como externo pueden ser tanto AH como ESP. En la Figura 25 se indica de manera gráfica la combinación entre túneles.

Figura 25 Combinación Entre Túneles, Caso 3



Fuente: RFC 2401

3.4.1.5 Gestión de las SA´s

El soporte de una SA establece los requerimiento mínimos para implementar seguridad en el entorno IPSec, se puede realizar de manera manual cuando se tiene ambientes pequeños y poco escalables además que se encuentren bajo un mismo dominio administrativo con un manejo de claves simétricas, por otro lado emplea soporte automático cuando se tiene un entorno escalable, por defecto usa el protocolo de intercambio de claves de Internet (IKE), para establecer una SA entre dos puntos; además se requiere llevar una gestión criptográfica de las claves para establecer parámetros comunes de algoritmo de cifrado tanto en el emisor como el receptor.

3.4.1.6 Protocolo de Cabecera de Autenticación (AH)

La cabecera de autenticación conocida por sus siglas en ingles AH, es empleada para brindar integridad orientada a no conexión y la autenticación en el origen de datos a las partes de la cabecera IP, así protege los datos de los protocolos de capas superiores; como un servicio opcional que provee AH es la protección contra reenvíos, llamando también anti-replay.

3.4.1.7 Formato de la Cabecera de Autenticación

Para añadir el protocolo de autenticación AH se requiere que en el campo Next Header de la cabecera del paquete IPv6 debe tener un valor de 51, cuyo valor se encuentra en el RFC 2402 y a su vez definido por la IANA.

La cabecera de autenticación AH está formada por ocho campos obligatorios, en la figura 26 se puede apreciar la estructura de la cabecera de autenticación.

Figura 26 Formato de la Cabecera de Autenticación AH

Fuente: RFC 2402

Cabecera Siguiente.- Este campo es de 8 bits, cuya función es identificar el tipo de carga o el tipo de cabecera de extensión que debería ir después de la cabecera de autenticación. El valor para este campo es elegido de un conjunto de números del protocolo IP que se encuentra definido en el RFC de números asignados en la IANA.

Longitud de Carga.- El tamaño de este campo es de 8 bits donde se indica la longitud de AH en palabras de 32 bits menos dos bits.

Reservado.- Este campo es de 16 bits cuyo propósito es de uso en el futuro con un valor fijado en cero.

Índice de Parámetro de Seguridad (SPI).- En este campo se coloca un número arbitrario de 32 bits, que trabaja en conjunto con la dirección de destino y el protocolo de seguridad AH para identificar una SA para cada paquete. Con propósito de usar en un futuro la IANA ha reservado el rango de 1 a 255 y el valor de cero para uso local.

Número de Secuencia.- El tamaño para este campo es de 32 bits, este es un número secuencial de manera ascendente con un contador inicializado en cero cuando se establece una SA. Este campo es obligatorio así el receptor, no lo

haya habilitado el servicio anti-replay, si este se habilita el transmisor da el número de secuencia; pero no se debe permitir que el número de secuencia retorne a cero.

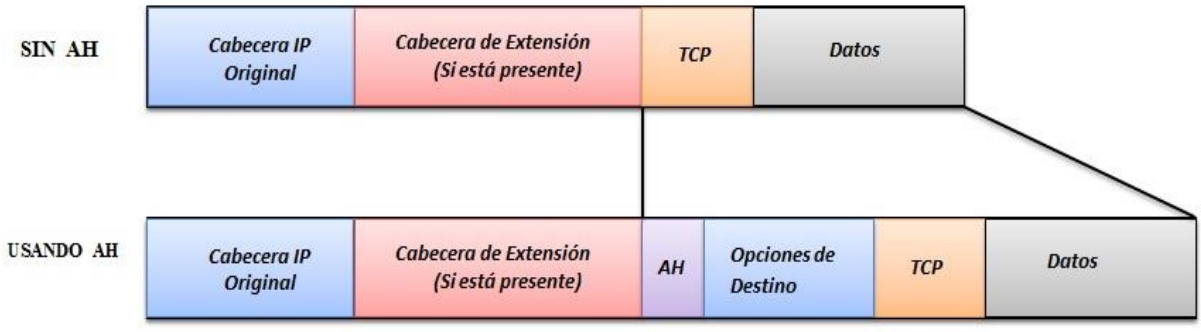
Datos de Autenticación.- El tamaño del campo es de longitud variable, es este campo contiene el valor de comprobación de integridad o conocido por las siglas en ingles ICV para el paquete especifico.
Además se puede incluir un relleno explicito cuyo propósito es asegurar que la longitud de la cabecera AH y este sea múltiplo entero de 64 bits en IPv6 y de 32 bits para IPv4.

3.4.1.8 Localización de la Cabecera de Autenticación

La cabecera de autenticación trabaja tanto en modo trasporte como en modo túnel.

En modo transporte la cabecera AH es insertado después de la cabecera IP y antes del campo del protocolo de capa superior en el caso de IPv6 la ubicación de la cabecera AH debe ir después de la o las cabeceras de extensión si es empleado, y la cabecera de extensión de destino puede estar antes o después de la cabecera AH. En la figura 27 se indica la ubicación de la cabecera AH en modo trasporte en el paquete IPv6.

Figura 27 Localización de la cabecera de autenticación en modo transporte



Fuente: RFC 2402

En modo túnel la función de la cabecera AH es proteger el paquete IP interno completamente ya que este paquete trasporta la última dirección tanto de origen y de destino, además protege al paquete IP externo quien contiene varias la dirección IP

como las direcciones de las pasarelas de seguridad. La ubicación de la cabecera AH en modo túnel dentro del paquete IPv6 se indica en la figura 28.

Figura 28 Localización de la cabecera de autenticación en modo túnel

Fuente: RFC 2402

3.4.1.9 Algoritmos de AH

Para brindar seguridad al paquete se emplea adicionalmente algoritmos de encriptación, con el propósito que la información al ser transportada desde el emisor hacia el receptor no sea modificada a esto se llamada también integridad de la información, para lo cual el protocolo AH emplea el algoritmo HMAC.

Hashed Message Authentication Code

Conocido por sus siglas en ingles HMAC, es un mecanismo de autenticación de mensajes cuyo objetivo es proteger la integridad de la información al ser transmitida, empleando la función hash que es una clave pública de longitud fija y única que se genera a partir de un mensaje de entrada de cualquier longitud y dicho resultado se le conoce como resumen que no es más que una huella que está asociada al paquete IP, además de una clave simétrica secreta que se encuentra ubicada en la cabecera y en el contenido IP.

En el receptor se realiza el cálculo de resumen del paquete recibido y comparará con el resumen del emisor si estas dos iguales indican que la integridad del paquete no ha sido modificada en el transporte de un extremo a otro.

3.4.1.10 Protocolo de Carga de Seguridad Encapsulada (ESP)

El protocolo de Carga de Seguridad Encapsulada o por su siglas en ingles ESP está referida en el RFC 2406; este protocolo brinda servicios de seguridad que puede ser empleado solo o en combinación del protocolo de la cabecera AH dentro de un escenario de un par de hosts, en un par de pasarelas de seguridad o entre un host y una pasarela de seguridad.

ESP proporciona el servicio de autenticación del origen de los datos, la integridad orientada a la no conexión estos dos servicios vienen unidos y se los denomina de manera general como autenticación; el servicio de anti-replay puede ser seleccionado sí o solo sí el servicio de autenticación del origen de datos ha sido seleccionado y es dependiente del receptor, ya que este controla el número de secuencia. Además brinda el servicio de confidencialidad limitada del flujo de tráfico este último servicio de seguridad es seleccionado independientemente de los otros servicios anteriormente mencionados, tanto la confidencialidad y la autenticación son opcionales pero al menos debe estar una de ellas seleccionadas.

3.4.1.11 Formato de Carga de Seguridad Encapsulada ESP

Para indicar que se empleará el protocolo de Carga de Seguridad Encapsulada ESP, se requiere que en el campo Next Header de la cabecera del paquete IPv6 debe tener un valor de 50 cuyo valor se encuentra en el RFC 2406 y a su vez definido por la IANA. En la figura 29 se muestra el formato de la cabecera de Carga de Seguridad Encapsulada.

Figura 29 Formato de la cabecera de carga de seguridad encapsulada ESP

Fuente: RFC 2406

Índice de Parámetros de Seguridad (SPI).- Es un número arbitrario de 32 bits dentro del rango de 1 a 255, cuyo objetivo es identificar a la Asociación de Seguridad conjuntamente a la con la dirección de destino IP y el protocolo de seguridad (ESP).

Número de Secuencia.- El tamaño para este campo es de 32 bits, este es un valor secuencial ascendente y único contador inicializado en cero cuando se establece una SA. Este campo es obligatorio y debe estar presente en el lado de transmisor incluso si el receptor no lo haya habilitado el servicio anti-replay por lo que el transmisor debe trasmitir este valor.

Datos de la carga útil.- El tamaño del campo es de longitud variable en números de bytes enteros y obligatorio, es aquí donde contiene los datos detallados por el campo Siguiente Cabecera o Next Header.

Longitud de Relleno.- Este campo es obligatorio e indica el número de bytes de relleno que se empleará el rango válido es de 0 a 255 bytes, si el valor es cero indica que no hay bytes de relleno.

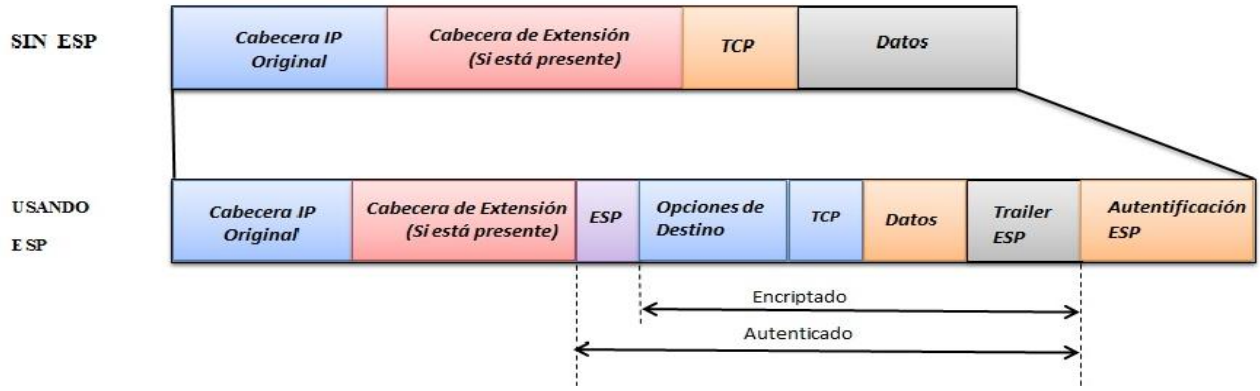
Siguiente Cabecera.-El tamaño de este campo es de 8 bits, este identifica el tipo datos que contiene en el campo de la carga útil. Para el valor de este campo se elige del conjunto de la RFC de Números Asignados que se encuentra dados para la IANA.

Datos de Autenticación.- Este campo es opcional y de longitud variable donde su longitud se encuentra en función de la autenticación que se ha seleccionado. Aquí se coloca el valor de comprobación de integridad conocido por las siglas ICV, este valor es calculado sobre el paquete ESP menos los datos de autenticación.

3.4.1.12 Localización de la Cabecera ESP

En el modo transporte la cabecera ESP se inserta después de la cabecera IP y antes del protocolo de la capa superior. En el caso de IPv6 la cabecera ESP va después de la o las cabeceras de extensión por el motivo que ESP en el modo transporte trabaja como carga útil de extremo a extremo, en el caso de la cabecera de extensión Opciones de Destino puede estar antes o después de la cabecera ESP, pero es preferible colocar después de la cabecera ESP, por la razón que este protocolo protege los campos que están después de esta. En la figura 30 se puede observar el orden de los campos cuando se emplea el protocolo de carga de seguridad encapsulada.

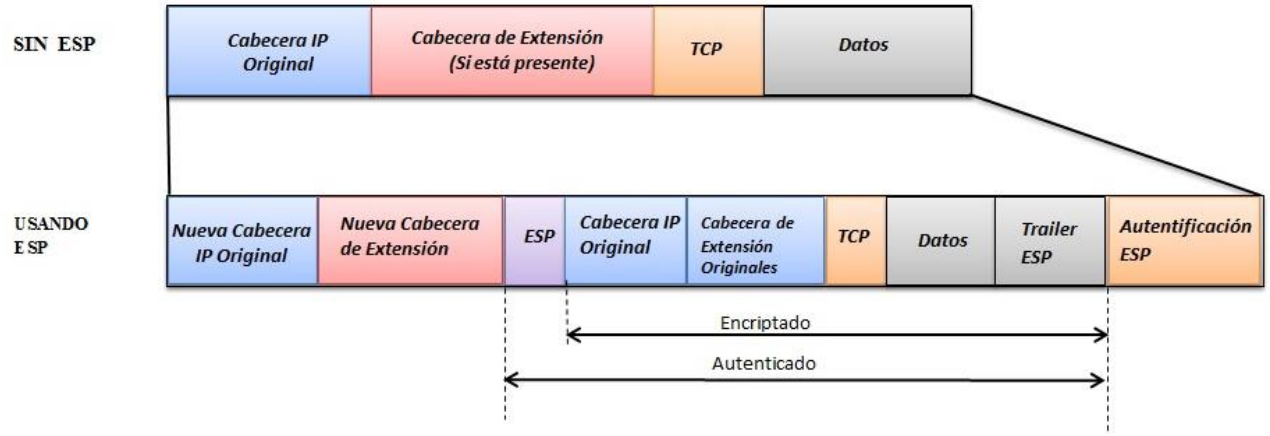
Figura 30 Localización de la cabecera ESP en modo transporte



Fuente: RFC 2406

En modo túnel, la función que cumple ESP es proteger al paquete IP interno completamente ya que este lleva las últimas direcciones de origen y de destino, mientras que la protección de la cabecera externa IP la cual contiene direcciones IP distintas, el comportamiento del protocolo ESP es el mismo que en modo transporte, el orden de los campos se aprecia en la figura 31.

Figura 31 Localización de la cabecera ESP en modo túnel



Fuente: RFC 2406

3.4.1.13 Algoritmos de ESP

ESP emplea algoritmos de encriptación debido a que el paquete podría llegar en desorden, además emplea de algoritmos autenticación de mensajes para la protección del paquete IP. Los cuales se encuentran basados en algoritmos simétricos o funciones hash.

La integridad de la información se logra utilizando una clave simétrica la cual es secreta y compartida, logrando así tener integridad de la información dentro del trayecto del emisor hacia el receptor, pero sí este es interceptado, se obtendrá un conjunto de bits ininteligibles ya que los datos fueron encriptados. Para determinar cuál de los dos protocolos de IPSec se empleará para la implementación en la infraestructura de la red donde en la tabla 4 se resalta puntos importantes acerca de sus características para brindar seguridad.

Tabla 4 Comparación entre los protocolos AH y ESP

AH	ESP
Brinda integridad y autenticación al paquete IP.	Brinda servicios de seguridad que puede ser empleado solo o en combinación del protocolo de la cabecera AH
Protege la carga útil del paquete IP y todos los campos del paquete IP incluyendo los protocolos de capas superiores.	Proporciona autenticación y cifrado a la carga útil del paquete IP y como servicio adicional brinda confidencialidad.
No proporciona ninguna garantía de confidencialidad, por lo tanto los datos transmitidos pueden ser vistos por terceros. (Pérez, 2001, pág. 52)	La cabecera IP no está protegida por el protocolo ESP por motivo que protege los campos que se encuentran después de la cabecera ESP.
Provee la protección contra reenvíos o llamados anti-replay.	El servicio de anti-replay puede ser seleccionado si el servicio de autenticación ha sido seleccionado y es dependiente del receptor ya que este controla el número de secuencia.
Emplea funciones hash y una clave simétrica compartida para la autenticación de mensajes.	Emplea algoritmos de encriptación y autenticación con una clave simétrica compartida dando como resultado robustez en la seguridad del paquete .
AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IPexcepto los "campos mutantes", es decir, aquéllos que pueden ser alterados en el tránsito y, por tanto, no autenticados (Yángüez, 2012, pág. 31)	La carga útil del paquete IP se transporta de manera encriptado.
Trabaja tanto en modo transporte y modo túnel.	Trabaja tanto en modo transporte y modo túnel.

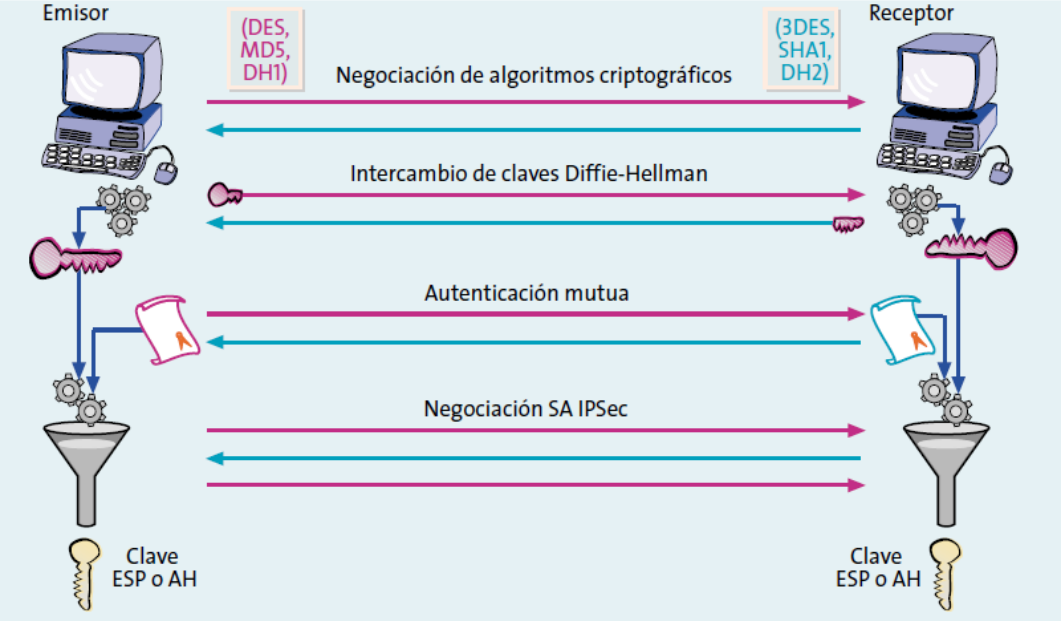
Elaborado por: Berenice Arguero

3.4.2 Protocolo de Internet Key EXchange (IKE)

Este es un protocolo hibrido cuyo propósito es negociar y proveer autenticación de claves para las asociaciones de seguridad de una manera protegida por lo tanto este no es un protocolo que viene incluido en IPSec, sino que ayuda al manejo de claves que se encuentra referido en el RFC 2409.

IKE por sus siglas en ingles de Internet Key Exchange es implementado en escenarios que necesita negociaciones entre dos extremos como, en redes privadas virtuales las VPN's, o en usuarios remotos, el cual tiene como objetivo negociar parámetros para establecer un SA mediante una conexión autenticada y cifrada, dicha negociación cumple con dos fases: la primera es crear un canal que sea seguro y autenticado para finalmente negociar los parámetros se seguridad o los parámetros que sean necesarios. En la figura 32 se indica la negociación de los parámetros de seguridad de IKE, obteniendo una clave de sesión, empleado en la protección de las conexiones de los protocolos ESP como AH.

Figura 32 Negociación de los parámetros de seguridad de IKE



Fuente: (Pérez, 2001, pág. 57)

Para el manejo de llaves emplea tres elementos que son OAKLEY, SKENE, ISAKMP cumpliendo con diferentes funciones que se mencionan a continuación:

OAKLEY.- Este protocolo define una serie de modos de intercambio de claves y detallando los servicios que provee cada uno de ellos, el cual se encuentra referido a la RFC 2412.

SKENE.- La función de este protocolo es describir una técnica de intercambio de claves de manera versátil brindando anonimato, repudio y cambio constante de claves.

ISAKMP.- Proporciona autenticación e intercambio de claves además está diseñado para soportar diferentes intercambios de llaves ya que este es independiente. Este protocolo indica las fases a seguir para brindar estos servicios de seguridad.

IPSec emplea para el manejo de llaves ISAKMP, con el propósito que el protocolo AH como ESP puedan brindar autenticación e integridad de la información en el envío de los paquetes IP; en una infraestructura Cisco, este protocolo trabaja con un mejor desempeño.

ISAKMP

Internet Security Association and Key Management Protocol conocido por sus siglas en ingles ISAKMP, es un protocolo criptográfico de gestión de SA´s, como la gestión de las claves cuya función es el mantenimiento de las claves, el cual se encuentra referido en el RFC 4306.

Este define los pasos necesarios para realizar la conexión de modo seguro del protocolo AH y del protocolo ESP como son: la creación y gestión de SA´s, la generación de claves para las SA´s y la autenticación entre pares, ya este protocolo requiere que toda la información que se intercambia sea cifrada y autenticada. (Yángüez, 2012, pág. 20)

CAPÍTULO 4
ANÁLISIS DE FACTIBILIDAD CON IPSEC

El Campus Sur cuenta con una extensión de internet 2, sin embargo esta aún no está integrada a la institución como un recurso adicional en la investigación, debido a que las aplicaciones y los proyectos que están siendo desarrollados en el laboratorio de SUN han sido objeto de manipulación, en razón a la falta de seguridad en esta red, esto conlleva a que se proponga implementar el protocolo de seguridad IPSec en el diseño tanto físico como lógico.

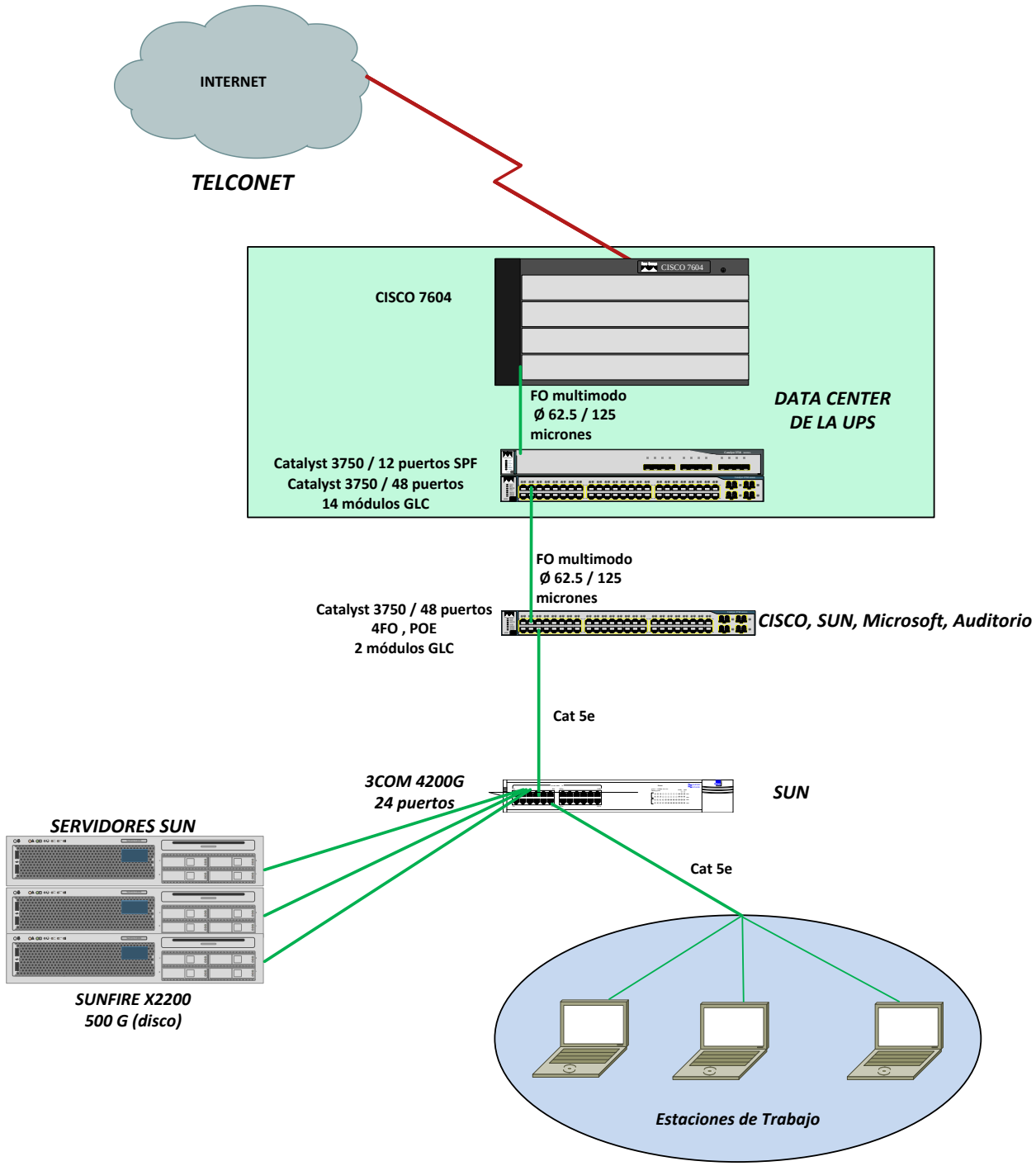
4.1 Diseño Físico

La conexión hacia la red avanzada a nivel nacional no se encuentra de manera directa, esta primero sale por internet comercial y de ahí se conecta al anillo de fibra óptica de Internet 2 a nivel nacional a través del proveedor TELCONET, empleando un router Cisco 7604.

El enlace hasta el laboratorio de SUN está compuesto por: un switch de core de la serie Catalyst 3750G POE-48, un switch de distribución de la serie Catalyst 3750 12 SPF, un switch de acceso de la serie Catalyst 3750G POE-48 para finalmente conectarse al laboratorio de SUN mediante un switch 3COM de la serie 4200G de 24 puertos de 1Gbps.

Adicionalmente cuenta con tres servidores SUN de la serie SunFire x2200 con 500 G de disco para cada uno de estos servidores, y con doce equipos donde desarrollan dichas aplicaciones para la rede avanzada. En la figura 33 se muestra la topología física de la red avanzada de la UPS Sede Quito Campus Sur.

Figura 33 Topología Física de la Red Avanzada de la UPS Sede Quito Campus Sur



Fuente: Universidad Politécnica Salesiana
Elaborado por: Berenice Arguero

4.2 Diseño Lógico

La conexión hacia la red avanzada CEDIA se realiza a través del proveedor Telconet, y a la UPS Sede Quito Campus Sur está asignada la dirección IPv6 2800:68:16::/48.

A partir de la dirección 2800:68:16::/64, ya se ha realizado el direccionamiento de las distintas VLAN´s de la institución; como estudio sólo se toma en cuenta la VLAN de internet 2, la VLAN de internet local y la VLAN de SUN.

Al no tener una conexión directa con la red CEDIA, todo el tráfico proveniente de la VLAN 16 deberá salir por la VLAN del internet local, que se encuentra conectada entre al switch de core y el router de Telconet. En la tabla 5 se indica las direcciones IPv6 correspondientes a las VLAN´S de: internet local, Telconet, y de SUN y el número de VLAN´s.

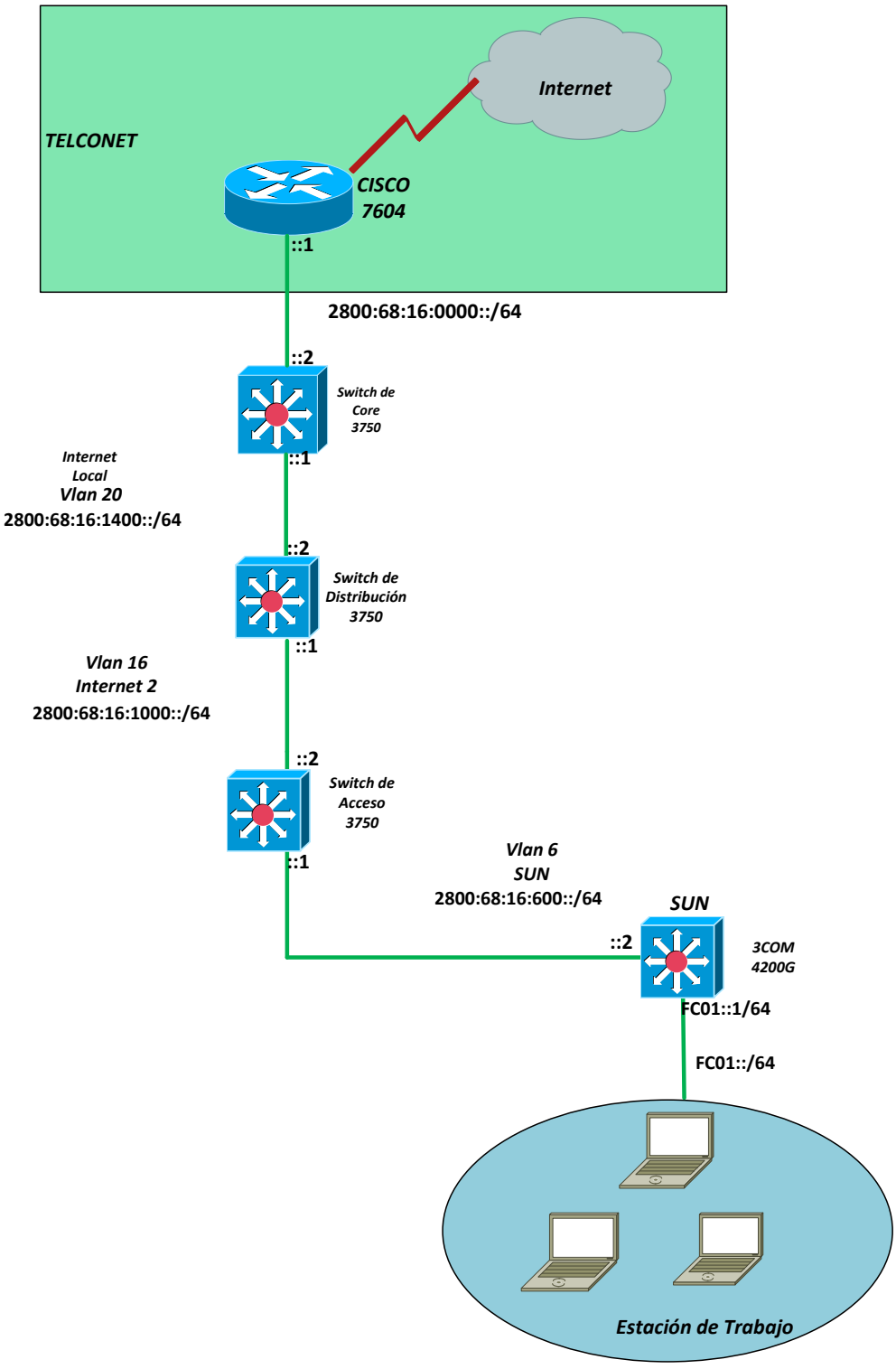
Tabla 5 Tabla de Direccionamiento de Internet 2 de la UPS

Nombre de la VLAN	N° VLAN	Dirección	Prefijo
Telconet	16	2800:68:16:1000::	/64
Internet local	20	2800:68:16:1400::	/64
SUN	6	2800:68:16:600::	/64

Fuente: (Moreno & Valencia, 2012, pág. 34)

En la figura 34 se puede apreciar el esquema de direccionamiento de la red avanzada desde el router CISCO 7604, hasta la estación de trabajo en el Laboratorio de SUN.

Figura 34 Topología Lógica de la Red de Internet 2 de la UPS Sede Quito Campus Sur



Fuente: Universidad Politécnica Salesiana
Elaborado por: Berenice Arguero

4.3 Simulación de la Implementación de IPSec

Para la simulación de implementación de IPSec para la red avanzada de la UPS Sede Quito Campus Sur se empleará el emulador gráfico gratuito conocido como GNS3 en el que se puede realizar redes complejas dentro de un entorno virtual. Una de las características principales de este programa es trabajar con dispositivos CISCO, que ejecutan diferentes IOS reales, empleando una plataforma llamada Dynamips y es quien proporciona el entorno gráfico.

Dynamips es un emulador de routers Cisco especialmente las series: 1700, 2600, 3600, 3700 y 7200 con sus correspondientes IOS estándar. Se puede mencionar las siguientes ventajas sobre otros simuladores.

- Se emplea como una plataforma de entrenamiento, para familiarizarse con dispositivos Cisco a través de un software del mundo real.
- Permite verificar configuraciones rápidamente que serán implementadas en escenarios reales. (GNS3, 2009, pág. 2).

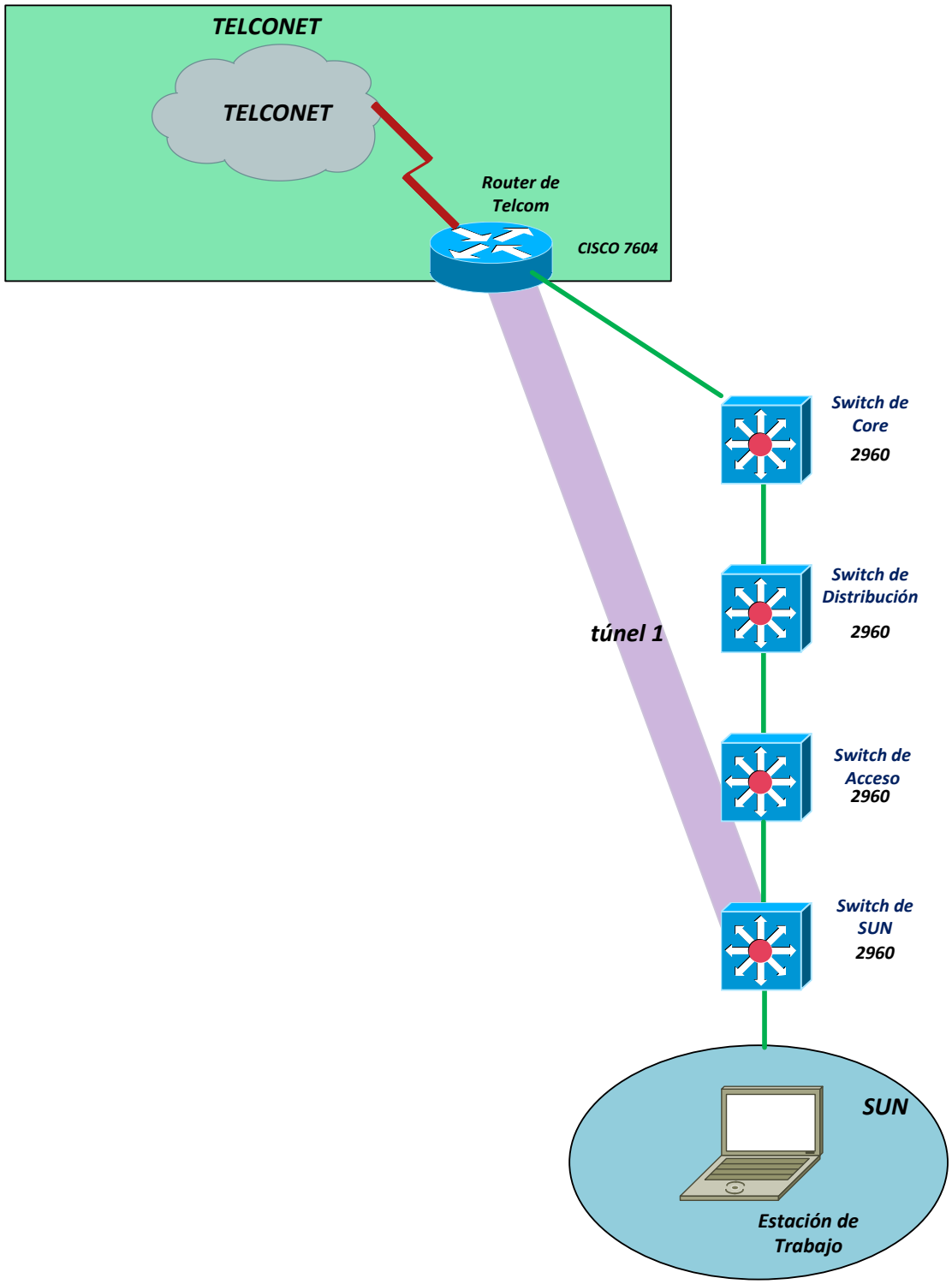
GNS3 tiene incluido programas como: Qemu, Pemu y VirtualBox los cuales permiten un trabajo conjunto entre un entorno virtual y un entorno real por ejemplo: Qemu es un emulador de máquina virtual que permite ejecutar cualquier sistema operativo completo, un software de prueba y aplicaciones que se encuentran dentro de una plataforma nativa de escritorio.

4.3.1 Diseño de Implementación del Protocolo IPSec

4.3.1.1 Diseño Físico

En cuanto a la topología física la conexión se realizará mediante la conexión por Ethernet entre cada uno de los switch desde la estación de trabajo hasta el router de Telconet. El escenario que se simulará se muestra en la figura 35.

Figura 35 Topología Física de Simulación para la Implementación de IPSec



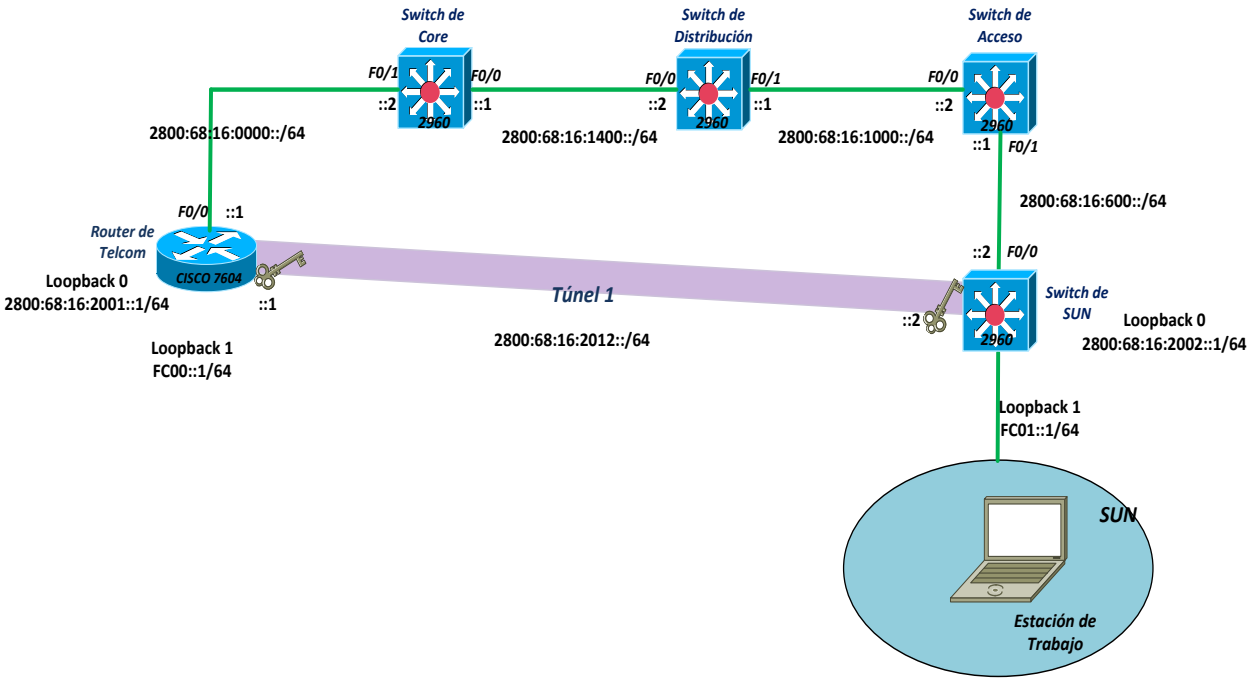
Fuente: Universidad Politécnica Salesiana
Elaborado por: Berenice Arguero

4.3.1.2 Diseño Lógico

La simulación de la red de internet 2 de la UPS se empleará switches de capa 3 de la serie Catalyst 2960 con su correspondiente IOS, remplazando el switch 3COM por un switch Catalyst 2960. La implementación del protocolo de seguridad IPSec se realizará entre dos dispositivos CISCO a través de una interfaz de túnel virtual con la finalidad de proteger el tráfico proveniente de la estación de trabajo de SUN hacia el router de frontera de Telconet.

Se añade dos interfaces viturales o loopback tanto el router Telconet como en el switch SUN, debido a que se requiere una de ellas para levantar el túnel entre estos dos dispositivos. Adicionalmente se realizará: el direccionamiento, el enrutamiento con el protocolo dinámico OSPF para luego proceder a la implementación del protocolo IPSec con los requerimientos correspondientes y se complementara con enrutamiento estático para el túnel. La topología lógica de simulación para la implementación de IPSec se observa en la figura 36.

Figura 36 Topología Lógica de Simulación para la Implementación de IPSec



Fuente: Universidad Politécnica Salesiana
Elaborado por: Berenice Arguero

Previamente a la implementación del protocolo de seguridad IPSec se debe crear la red como se muestra en la topología lógica, para proceder a realizar las configuraciones iniciales en cada uno de los dispositivos que son necesarias para la conectividad. Como contraseña se usa la palabra cisco y se utiliza las direcciones IPv6 que proporciona la tabla de direccionamiento para aplicarlas a cada una de las interfaces de los dispositivos. En la tabla 6 se indica la tabla de direccionamiento para las interfaces de cada uno de los dispositivos, y se incluye el IOS que se utilizará en la simulación.

Tabla 6 Tabla de Direccionamiento

Nombre del Switch	Interfaz	Dirección IPv6	IOS
RTelconet	F 0/0 Loopback 0 Loopback 1	2800:68:16:0000::1/64 2800:68:16:2001::1/64 FC00::1/64	c2691-advipservicesk9-mz.124-15.T6
SwCore	F 0/1 F 0/0	2800:68:16:0000::2/64 2800:68:16:1400::1/64	c2691-advipservicesk9-mz.124-15.T6
SwDistribucion	F 0/0 F 0/1	2800:68:16:1400::2/64 2800:68:16:1000::1/64	c2691-advipservicesk9-mz.124-15.T6
SwAcceso	F 0/0 F 0/1	2800:68:16:1000::2/64 2800:68:16:600::1/64	c2691-advipservicesk9-mz.124-15.T6
SwSUN	F 0/0 Loopback 0 Loopback 1	2800:68:16:600::2/64 2800:68:16:2002::1/64 FC01::1/64	c2691-advipservicesk9-mz.124-15.T6

Fuente: Universidad Politécnica Salesiana
Elaborado por: Berenice Arguero

Los requerimientos para la configuración del protocolo de seguridad IPSec se muestra en la tabla 7 como son: la dirección IPv6 de la interfaz del túnel, la clave que es la contraseña compartida, el algoritmo de cifrado, el algoritmo hash, el método de autenticación y el tiempo de vida de la IKE.

Tabla 7 Requerimientos para la Implementación de IPSec

Dispositivo	Router Telcom	Switch SUN
Protocolo IPSec	✓	✓
Dirección IPv6 Túnel 1	2800:68:16:2012::1/64	2800:68:16:2012::2/64
Enrutamiento Túnel 1	estático	Estático
Clave	hh87fkqwfw	hh87fkqwfw
Algoritmo de Cifrado	3DES	3DES
Algoritmo Hash	MD5	MD5
Intercambio de Llaves	Diffie-Hellman Grupo 1 de 768 bits	Diffie-Hellman Grupo 1 de 768 bits
Método de Autenticación	Pre-share	Pre-share
Tiempo de vida IKE	86400 segundos	86400 segundos

Fuente: Jorge López (2013)

4.3.2 Configuración Básica

A cada uno de los dispositivos tanto al router de TELCONET como los switches de capa tres se realizó la configuración básica con los siguientes parámetros:

- Configuración del nombre de cada uno de los dispositivos
- Desactivación de la búsqueda del DNS
- Configuración de un mensaje de bienvenida
- Configuración de la contraseña de modo EXEC
- Configuración de la contraseña de consola
- Configuración de la contraseña para las líneas de terminales virtuales
- Configuración de las interfaces

El enrutamiento dinámico se aplica el protocolo OSPF para IPv6 puesto que este proporciona soporte de autenticación y protección de IPSec. A continuación se muestra la configuración básica de uno de los dispositivos de la topología debido a que la configuración se realizó para cada uno de ellos y con la dirección IPv6 correspondiente a cada interface.

Configuración Básica del Router Telconet

```
RTelconet(config)#no ip domain-lookup                // Desactiva  la búsqueda del DNS
RTelconet(config)#enable secret cisco                // Configura  la contraseña de modo
EXEC
RTelconet(config)#banner motd “AUTORIZADO”  // Mensaje de Bienvenida
RTelconet(config)#line console 0                     // Configura la contraseña de consola
RTelconet(config)#password cisco
RTelconet(config)#login
RTelconet(config)#loggin synchronous        //Evita que los mensajes IOS enviados a las líneas
                                              de consola o Telnet interrumpan la entrada por
teclado.
RTelconet(config)#exit
RTelconet(config)#line vty 0 4               // Configura la contraseña de las líneas terminales
RTelconet(config)#password cisco
RTelconet(config)#login
RTelconet(config)#loggin synchronous
RTelconet(config)#exit
RTelconet(config)# interface fastethernet 0/0 // Se especifica la interfaz de configuración
RTelconet(config-if)#  ipv6 enable                                  // Activa el protocolo IPv6
RTelconet(config-if)# ipv6 address 2800:68:16:0000::1/64    // Asignación de la dirección
ipv6 a
                                                                    la interface
RTelconet(config-if)# no shutdown                           // Habilita la interface
RTelconet(config-if)# exit
```

Configuración de OSPF para IPV6

```
RTelconet(config)# ipv6  unicast-routing             // Habilita el ruteo IPv6
RTelconet(config)# interface fastethernet 0/0        // Se especifica la interfaz de
configuración
                                                       para el OSPF
RTelconet(config-if)# ipv6 ospf 1 area 0             // Habilitando OSPF IPv6 con valor  1
para
                                                       el process id y el valor de 0 para el
área.
RTelconet(config)# router-id 10.1.1.1                // Establece una identificación para el
                                                       proceso de ruteo
```

4.3.3 Configuración de Protocolo IPSec

En primera instancia hay que crear las políticas IKE asigna una prioridad única del 1 al 10000 siendo el número uno la prioridad más alta (Cisco Systems, Inc., 2012, pág. 5), aquí se establecen los parámetros de seguridad que se utilizará para proteger las negociaciones que se empleará una vez que las dos partes se han puesto de acuerdo, estos parámetros se identifican por una SA que son aplicados durante toda la negociación. Una vez creado la política IKE se establece la identidad de ISAKMP que es la dirección IPv6 de los pares para que cada dispositivo envíe su identidad al par remoto.

La negociación empieza cuando un dispositivo busca una coincidencia en la política se seguridad que ha recibido del otro par y la compara con la su suya, los dos pares deben tener los mismos parámetros de: encriptación, autenticación, hash, valores de Diffie-Hellman, y el tiempo de vida de la SA, si el tiempo de vida no es idéntico se utiliza el más corto completando la negociación, si se encuentra una coincidencia entre las políticas de los pares y se creará las asociaciones de seguridad IPSec caso contrario se negará la negociación IKE por lo tanto no se establecerá IPSec.

Los parámetros que se emplearán para la implementación de IPSec son: para el algoritmo de cifrado 3DES, para la autenticación el algoritmo hash MD5 en vista de que este garantiza la integridad de los datos, por otra parte para el intercambio de llaves se empleará Diffie-Hellman grupo 1, dado que Diffie-Hellman está dividido en tres grupos por la fortaleza de las claves, el grupo 1 proporciona seguridad básica además de un buen rendimiento con un identificador de 768 bits, los grupos 2 y 5 para un identificador de 1024 bits y 1536 bits correspondientemente, estos ofrecen una seguridad más efectiva sin embargo su rendimiento es pobre dentro de un túnel debido a la velocidad de intercambio de llaves. (About Diffie-Hellman Groups, 2010).

Como tiempo máximo de vigencia para una política de seguridad se emplea 86400 segundos o un día.

Configuración del Router Telconet (Shirkar, 2013)

a. Configuración de las Políticas IKE

```
RTelconet(config)# crypto isakmp policy 1          // Crea una nueva política con la prioridad
RTelconet(config-isakmp)# authentication pre-share // Establece el método de autenticación
RTelconet(config-isakmp)# hash md5                 // Establece el algoritmo hash
RTelconet(config-isakmp)# group 1                  // Especifica el método de intercambio de
                                                      llaves del grupo Dieffe-Hellman
RTelconet (config-isakmp)# encryption 3des         // Establece el método de encriptación
RTelconet (config-isakmp)# lifetime 86400          // Especifica el tiempo de vida de la SA
RTelconet (config-isakmp)#exit
```

b. Configuración de las Claves pre-compartidas

RTelconet(config)# crypto isakmp key 0 ipsecvpn address ipv6 2800:68:16:2002::1/64 // Se define la clave pre-comparida, con la dirección ipv6
RTelconet(config)# crypto keyring I2UPS // Se define el nombre de la clave que se usará durante la autenticación.
RTelconet(config-keyring)# pre-shared-key address ipv6 2800:68:16:2002::1/64 key 87fkqwfw // Se define la clave pre-compartida con la dirección
RTelconet(config-keyring)#exit

c. Configuración IPSec Transform-Set

RTelconet(config)# crypto ipsec transform-set COMBINACION esp-3des esp-md5-hmac // Define un trasnsform-set que es una combinación de protocolos y algoritmos.
RTelconet(config)# mode tunnel // Especifica el modo de trabajo.
RTelconet(config)# exit

d. Configuración IPSec Profile

RTelconet(config)# crypto ipsec profile LISTA // Se define el nombre para los parámetros de seguridad.
RTelconet(config)# set transform-set COMBINACION // Especifica que conjuntos de transformación se pueden utilizar.
RTelconet(config)# exit

e. Configuración de ISAKMP Profile en IPv6

RTelconet(config)# crypto isakmp profile 3des // Define un perfil de ISAKMP y auditorías Sesiones de usuario IPsec.
RTelconet(conf-isa-prof)#self-identity address ipv6 // Define la identidad que el IKE locales utiliza para identificarse en el extremo remoto.
RTelconet(conf-isa-prof)#match identity address ipv6 2800:68:16:2002::1/64 // Especifica la identidad del dispositivo del otro extremo del túnel.
RTelconet(conf-isa-prof)#keyring I2UPS // Asocia la clave pre-compartida
RTelconet(conf-isa-prof)# exit

f. Configuración del Túnel e IPSec

RTelconet(config)# int tunnel 1 // Especifíca la interfaz del túnel y el número de entrada
RTelconet(config-if)# ipv6 enable
RTelconet(config-if)# ipv6 address 2800:68:16:2012::1/64 // Provee una dirección IPV6 al túnel
RTelconet(config-if)# tunnel source 2800:68:16:2001::1 // Define el origen para túnel
RTelconet(config-if)# tunnel destination 2800:68:16:2002::1// Define el destino para túnel
RTelconet(config-if)# tunnel mode ipsec ipv6 // Establece el modo de encapsulación para el túnel
RTelconet(config-if)# tunnel protection ipsec profile LISTA // Se asocia a la interfaz el túnel con el perfil IPSec.
RTelconet(config-if)# exit

g. Enrutamiento Estático

RTelconet(config)#ipv6 route FC01::/64 2800:68:16:2012::2 // Configura una ruta estática hacia la dirección loopback que representa la estación de trabajo, mediante la interfaz del tunel.

Configuración del Switch de SUN (Shirkar, 2013)

a. Configuración de las Políticas IKE

```
SwSUN(config)# crypto isakmp policy 1          // Crea una nueva política con la prioridad
SwSUN(config-isakmp)# authentication pre-share  // Establece el método de autenticación
SwSUN(config-isakmp)# hash md5                  // Establece el algoritmo hash
SwSUN(config-isakmp)# group 1                   // Especifica el método de intercambio de llaves del grupo Dieffe-Hellman
SwSUN(config-isakmp)# encryption 3des           // Establece el método de encriptación
SwSUN(config-isakmp)# lifetime 86400            // Especifica el tiempo de vida de la SA
SwSUN(config-isakmp)#exit
```

b. Configuración de las Claves pre-compartidas

```
SwSUN(config)# crypto isakmp key 0 ipsecvpn address ipv6 2800:68:16:2001::1/64   // Se define la clave pre-comparida, con la dirección ipv6
SwSUN(config)# crypto keyring I2UPS             // Se define el nombre de la clave que se usará durante la autenticación.
SwSUN(config-keyring)# pre-shared-key address ipv6 2800:68:16:2001::1/64 key 87fkqwfw
// Se define la clave pre-compartida con la dirección
SwSUN(config-keyring)#exit
```

c. Configuración IPSec Transform-Set

```
SwSUN(config)# crypto ipsec transform-set COMBINACION esp-3des esp-md5-hmac // Define un trasnsform-set que es una combinación de protocolos y algoritmos.
SwSUN(config)# mode tunnel      // Especifica el modo de trabajo.
SwSUN(config)# exit
```

d. Configuración IPSec Profile

```
SwSUN(config)# crypto ipsec profile LISTA       // Se define el nombre para los parámetros de seguridad.
SwSUN(config)# set transform-set COMBINACION // Especifica que conjuntos de transformación se pueden utilizar.
SwSUN(config)# exit
```

e. Configuración de ISAKMP Profile en IPv6

```
SwSUN t(config)# crypto isakmp profile 3des  // Define un perfil de ISAKMP y auditorías Sesiones de usuario IPSec.
```

SwSUN (conf-isa-prof)#self-identity address ipv6 // Define la identidad que el IKE locales utiliza para identificarse en el extremo remoto.
SwSUN (conf-isa-prof)#match identity address ipv6 2800:68:16:2001::1/64 // Especifica la identidad del dispositivo del otro extremo del túnel.
SwSUN(conf-isa-prof)#keyring I2UPS // Asocia la clave pre-compartida
SwSUN(conf-isa-prof)# exit

f. Configuración Túnel e IPSec

SwSUN(config)# int tunnel 1 // Especifica la interfaz del túnel y el número de entrada
SwSUN(config-if)# ipv6 enable
SwSUN(config-if)# ipv6 address 2800:68:16:2012::2/64 // Provee una dirección IPV6 al túnel
SwSUN(config-if)# tunnel source 2800:68:16:2002::1 // Define el origen para túnel
SwSUN(config-if)# tunnel destination 2800:68:16:2001::1// Define el destino para túnel
SwSUN(config-if)# tunnel mode ipsec ipv6 // Establece el modo de encapsulación para el túnel
SwSUN(config-if)# tunnel protection ipsec profile LISTA // Se asocia a la interfaz el túnel con el perfil IPSec.
SwSUN(config-if)# exit

g. Enrutamiento Estático

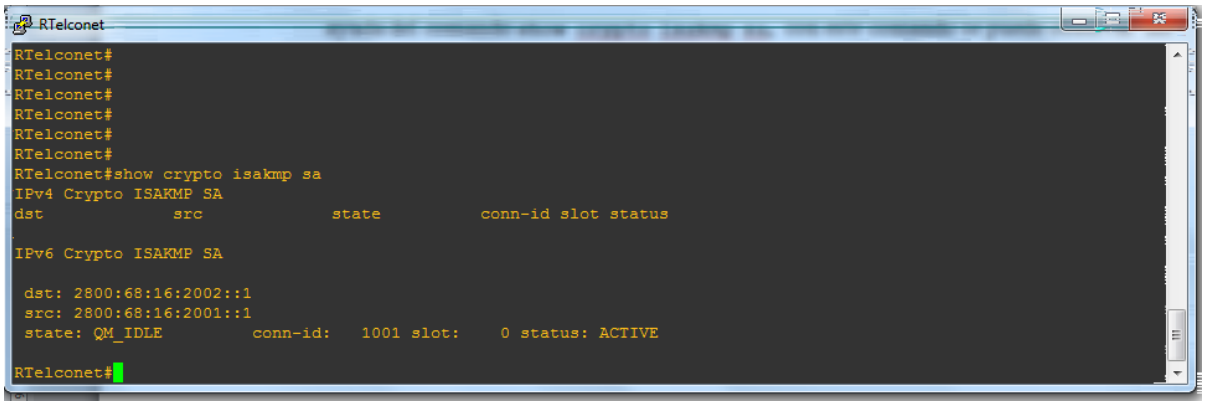
SwSUN (config)#ipv6 route FC00::/64 2800:68:16:2012::1 // Configura una ruta estática hacia la dirección loopback que representa la estación de trabajo, mediante la interfaz del tunel.

4.3.4 Verificación de la Operación de IPSec

Para la verificación de la operación del protocolo IPSec en la red propuesta, se emplea ciertos comandos, pero los principales son: `show crypto isakmp sa`, `show crypto engine connection active`, y `show crypto ipec sa`. (Cisco Systems, Inc., 2012, págs. 14-16)

Al usar el comando **`show crypto isakmp sa`**, se puede observar las sesiones ISAKMP que se encuentran activas en el router, también las asociaciones de seguridad de IKE como se observa en figura 37.

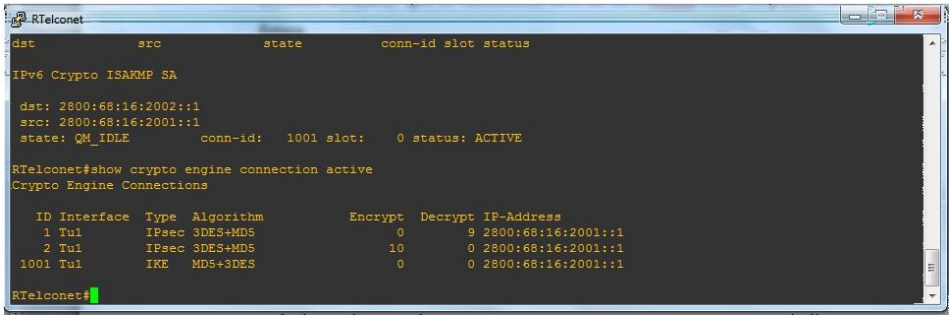
Figura 37 Resultado del comando show crypto isakmp sa



Fuente: Captura del programa GNS3

Así mismo el comando **`show crypto engine connection active`**, indica en resumen la información de configuración de la encriptación, además ayuda a verificar que el túnel está en funcionamiento. En la figura 38 se muestra las interfaces con los algoritmos de encriptación con las correspondientes direcciones IPv6. (Cisco Systems, Inc., 2012, págs. 14-16).

Figura 38 Resultado del comando *show crypto isakmp sa*



Fuente: Captura del programa GNS3

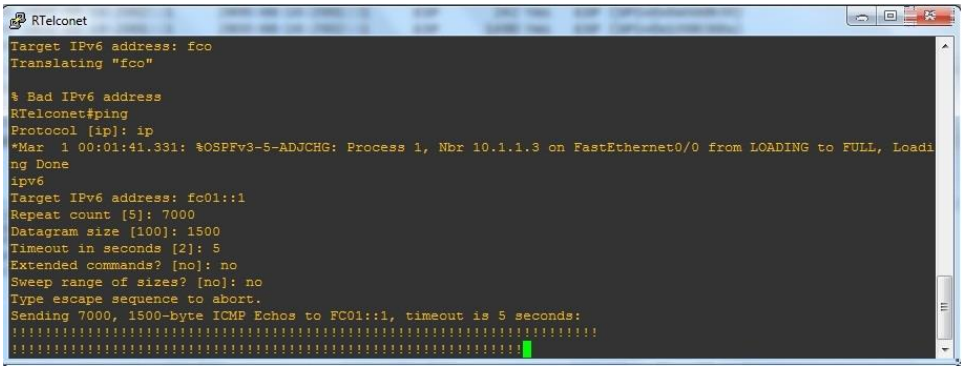
Al usar el comando **`show crypto ipec sa`**, muestra las asociaciones de seguridad que se encuentra en uso desde el router de Telconet hasta el switch de SUN.

```
RTelconet#show crypto ipsec sa
interface: Tunnel1
   Crypto map tag: Tunnel1-head-0, local addr 2800:68:16:2001::1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2800:68:16:2002::1 port 500
```

```
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
 local crypto endpt.: 2800:68:16:2001::1,
 remote crypto endpt.: 2800:68:16:2002::1
 path mtu 1514, ip mtu 1514, ip mtu idb Tunnel1
 current outbound spi: 0xC9634E7F(3378728575)
 inbound esp sas:
 spi: 0x33DD7B73(870153075)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 1, flow_id: SW:1, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4398904/2696)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
 inbound ah sas:
 inbound pcp sas:
 outbound esp sas:
 spi: 0xC9634E7F(3378728575)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2, flow_id: SW:2, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4398904/2694)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
 outbound ah sas:
 outbound pcp sas:
```

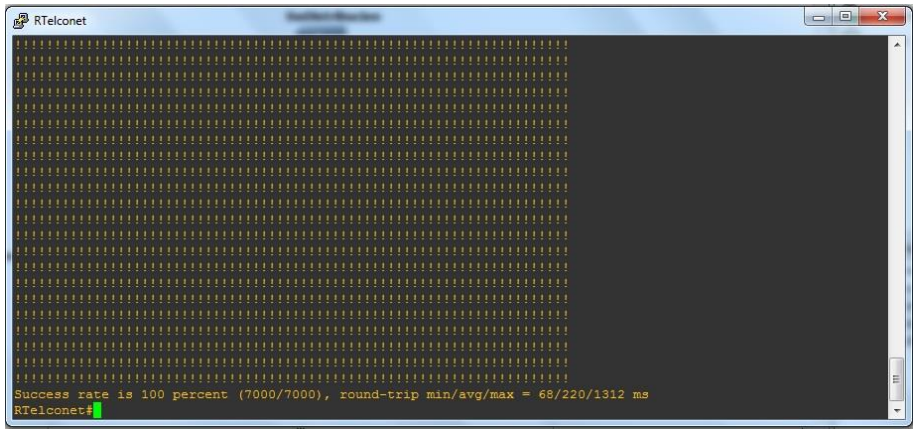
Finalmente se realizó la verificación de la conectividad desde el router de Telconet hacia la estación de trabajo que está representada por la red loopback FC01::1 como desde el Switch de Sun hasta la loobpack FC00::1, mediante un ping extendido ya que realiza una comprobación más avanzada, obteniendo los siguientes resultados favorables y que se indican en la figura 39 y en la figura 40.

Figura 39 Resultados del ping extendido desde el Router Telconet hacia FC01::1



Fuente: Captura del programa GNS3

Figura 40 Resultados del ping extendido desde el Router Telconet hacia FC01::1



Fuente: Captura del programa GNS3

Como resultado visible se tiene los puntos de exclamación el cual indica la recepción de una respuesta del ping, además se tiene una tasa de éxito del 100%, es decir no hubo pérdidas de paquetes de eco; un porcentaje de menos del 80% es considerando como un problema. (CISCO, 2006, págs. 4-5).

El tiempo de ida y vuelta por paquetes tiene un tiempo promedio de 220 ms de un punto al otro de manera encriptado.

4.4 Análisis de Resultados

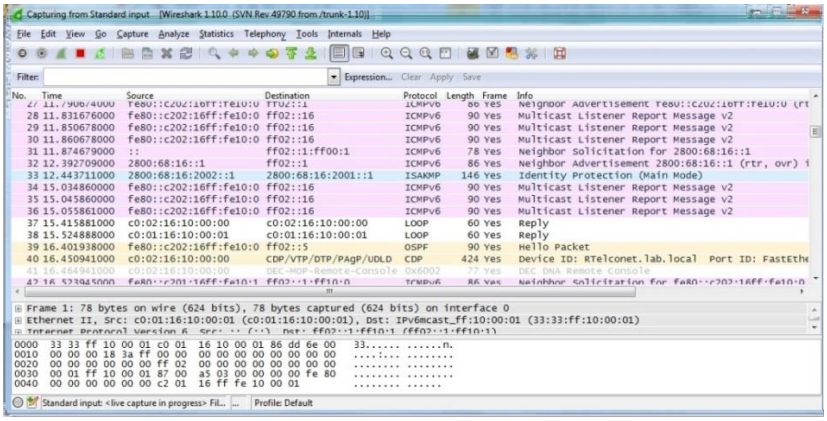
Se realizó un estudio comparativo entre un escenario con el protocolo de seguridad IPSec y sin él, en vista de que en un estudio anteriormente citado por los autores Rico

Dewar, Mediana Yurley y Santos Luz Mariana, indican que el uso de este protocolo puede causar una desmejora en el desempeño de la red por lo tanto debe ser empleado cuando se tiene que proteger a todo el tráfico caso contrario no es necesario implementarlo. (2008, pág. 325)

Esto se llevó a cabo a través de una herramienta gráfica llamada Wireshark, ya que identifica y analiza el tipo tráfico de la red en un determinado momento y de manera detallada. Una de sus innumerables funciones es la capacidad visualizar estadísticamente la información general o específico de un cierto protocolo, adicionalmente genera gráficos estadísticos de o los protocolos de motivo de estudio seleccionados, posibilitando desarrollar el análisis de resultado que se obtiene al implementar el protocolo de seguridad IPSec.

La captura de los paquetes se realizó en los dos escenarios de estudio desde el router denominado Telconet hasta el switch denominado SUN, cabe recalcar que dichas capturas fueron tomadas desde que se inicia los dispositivos de red hasta cuando culmina el ping extendido. Dentro del escenario de implementación del protocolo IPSec se logró revisar los paquetes ICMPV6, los paquetes "HELLO" del protocolo OPSF, los paquetes ISAKMP, y el protocolo ESP, donde los resultados de dichas capturas se emplearán en el análisis. La figura 41 muestra un ejemplo de las capturas de los diferentes paquetes.

Figura 41 Capturas de los diferentes paquetes mediante Wireshark



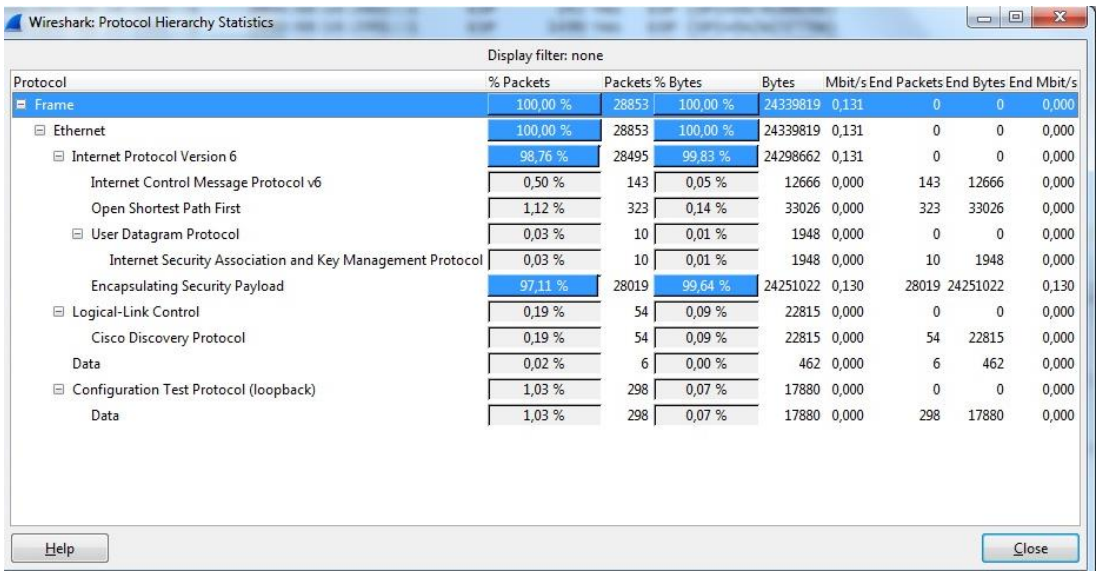
Fuente: Captura del programa Wireshark

Dentro del escenario de implementación del protocolo de seguridad, el porcentaje de paquetes transmitidos es de un 100% con un número total de 28853 paquetes, incluidos los paquetes: IPV6, ICMPV6, OSPF, ISAKMP, ESP.

El porcentaje de paquetes capturados del protocolo de IPv6 es del 98,76% transmitiendo 28495 paquetes, el cual está conformado por los siguiente protocolos: ICMPV6 transmitiendo 143 paquetes correspondiente al 0,50%, el protocolo OSPF transmitió 323 paquetes enviados que pertenece al 1,12%, el protocolo ISAKMP con 10 paquetes transmitidos con 0,03% y en último lugar el protocolo ESP con un número total de 28019 paquetes con un porcentaje correspondiente de 97,11% completando así el 98,76%.

Luego se observa que el protocolo de loopback usado en la creación del túnel, ha generado 298 paquetes, lo que equivale al 1,03%, adicionalmente el protocolo CISCO DISCOVERY generó 54 paquetes que corresponden al 0,19%. Los datos de la capa LLC representan un 0,02% y corresponden a total de 6 paquetes. Por consiguiente se obtiene el 100% de los paquetes capturados. Como se puede comprobar en la figura 42 con la herramienta Wireshark.

Figura 42 Ventana de Estadísticas de los Protocolos por Jerarquía



Fuente: Captura del programa Wireshak

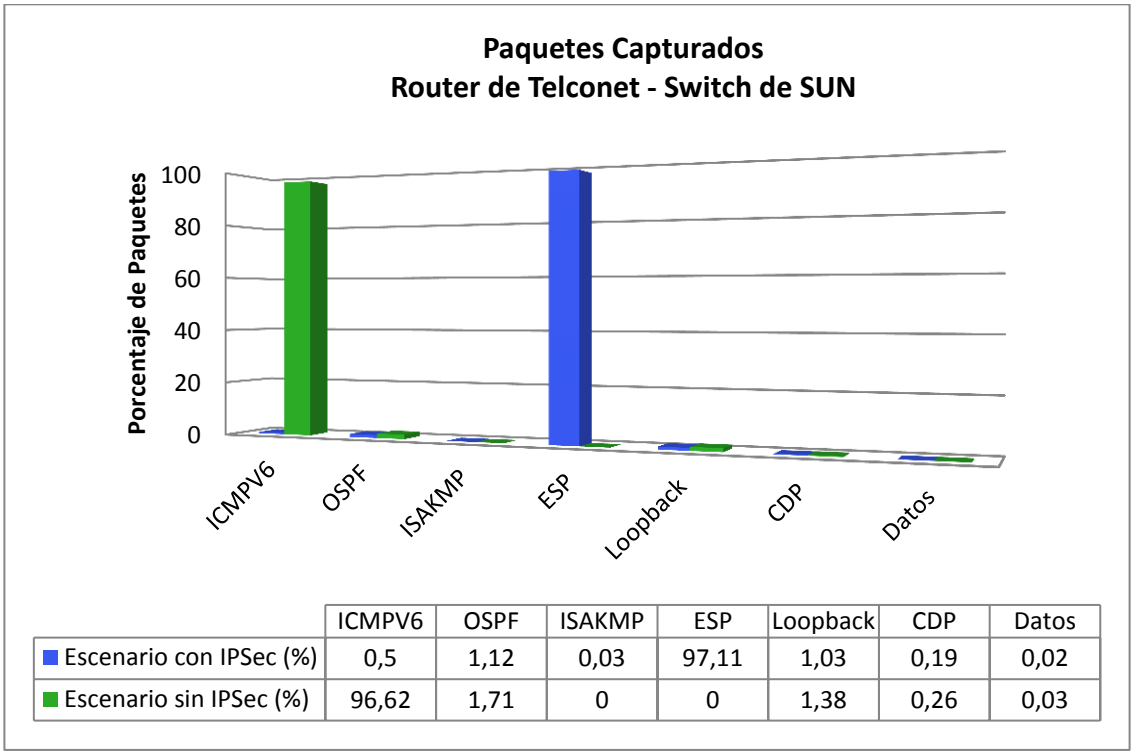
De igual manera se realizó la captura de los paquetes de los protocolos dentro del escenario de simulación sin el protocolo de IPSec, con su configuración necesaria y el enrutamiento anteriormente desarrollado, el cual cooperará en un análisis comparativo entre los dos escenarios. En la tabla 8 se muestra un resumen del porcentaje de los paquetes de los protocolos que fueron capturados en los dos escenarios de simulación y de acuerdo con los resultados obtenidos de estos dos casos de estudio se generó un cuadro estadístico de los paquetes capturados como se observa en la figura 43.

Tabla 8 Tabla comparativa en porcentaje de los paquetes capturados en los diferentes escenarios

Protocolos		**Escenario con IPSec (%)**	**Escenario sin IPSec (%)**
IPv6	ICMPV6	0,50	96,62
	OSPF	1,12	1,71
	ISKMP	0,03	___
	ESP	97,11	___
		98,76	98,33
Loopback	DATOS	1,03	1,38
Logical-link Control	CDP	0,19	0,26
Datos	DATOS	0,02	0,03
	Total	100 %	100 %

Elaborado por: Berenice Arguero

Figura 43 Cuadro estadístico del porcentaje de paquetes capturados de los diferentes protocolos



	ICMPV6	OSPF	ISAKMP	ESP	Loopback	CDP	Datos
Escenario con IPSec (%)	0,5	1,12	0,03	97,11	1,03	0,19	0,02
Escenario sin IPSec (%)	96,62	1,71	0	0	1,38	0,26	0,03

Elaborado por: Berenice Arguero

El análisis se emplea mediante la tabla 8, con el cual es posible determinar las diferencias entre los dos escenarios de simulación. Primero se hace referencia al porcentaje de paquetes capturados por los protocolos en cada caso. Al comparar estas evidencias existe una ligera diferencia del porcentaje del paquete IPv6, con el protocolo IPSec se trasmitieron el 98,76% de paquetes mientras que sin el protocolo se transmitió el 98,33% ,con una diferencia de 0,43%, sin embargo al desglosar los protocolos que conforman el protocolo IPv6 es notorio que dentro del escenario con IPSec hay una disminución del 92,12% de paquetes ICMPV6 en relación con el escenario sin IPSec, dado que el 0,50% simboliza los paquetes que se han empleado para el descubrimiento de vecinos de la red a través de mecanismos multicast como para el reporte de errores, mientras que 96,62% correspondiente al segundo caso representa el ping desde el router Telconet hasta el switch SUN. Como resultado de la implementación del protocolo de seguridad, se manifiesta con el 97,11% los paquetes ESP, los cuales están relacionados con el ping que se realizó de extremo a

extremo, considerándose que los paquetes enviados están encapsulados y encriptados por consiguiente se aumentó la seguridad. Adicionalmente se tiene una diferencia menor al 1% de paquetes de los protocolos de: Loopback por motivo que en el escenario con el protocolo IPSec se aumentó dos redes virtuales como apoyo para la creación del túnel, así como una ligera disminución del protocolo CDP y los datos.

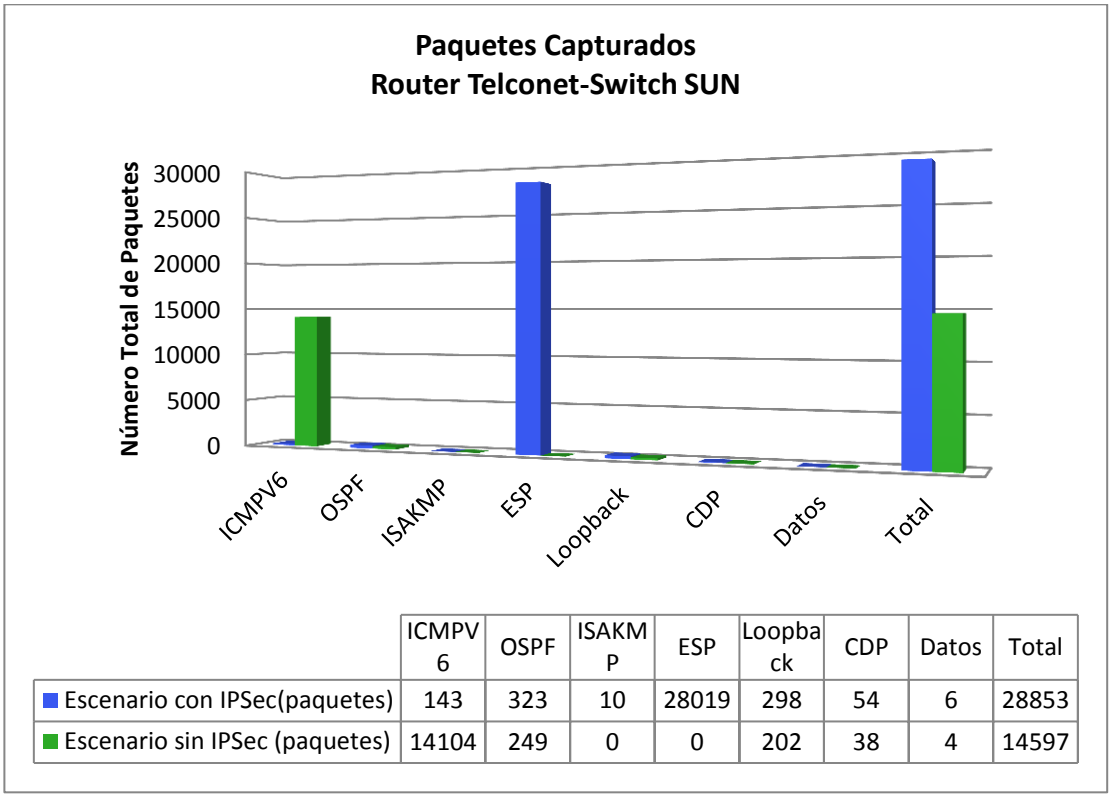
Si bien es cierto se considera una diferencia mínima de 0,43% correspondiente al porcentaje del protocolo IPv6 entre el escenario con IPSec y el escenario sin IPSec cuyo resultado es poco apreciable por la cantidad de paquetes que pasaron para evidenciar si hubo algún cambio al implementar el protocolo de seguridad IPSec, donde no es notorio el números de paquetes que fueron transmitidos. Para ello se toma en consideración el número total de paquetes de los protocolos transmitidos entre los dispositivos en los dos casos de estudio con apoyo de una de las herramientas Wireshak. Se ha elaborado una tabla comparativa del número de paquetes de los protocolos en los diferentes escenarios como se señala en la tabla 9, como complemento se manifiesta dichos resultados en un cuadro estadístico que se observa en la figura 44.

Tabla 9 Tabla comparativa del número de paquetes capturados en los diferentes escenarios.

Protocolos		**Escenario con IPSec (paquetes)**	**Escenario sin IPSec (paquetes)**
IPv6	ICMPV6	143	14104
	OSPF	323	249
	ISKMP	10	___
	ESP	28019	___
		28495	14353
Loopback	DATOS	298	202
Logical-link Control	CDP	54	38
Datos	DATOS	6	4
	Total	28853	14597

Elaborado por: Berenice Arguero

Figura 44 Cuadro estadístico del números de paquetes capturados de los diferentes protocolos



	ICMPV6	OSPF	ISAKMP	ESP	Loopback	CDP	Datos	Total
Escenario con IPSec(paquetes)	143	323	10	28019	298	54	6	28853
Escenario sin IPSec (paquetes)	14104	249	0	0	202	38	4	14597

Elaborado por: Berenice Arguero

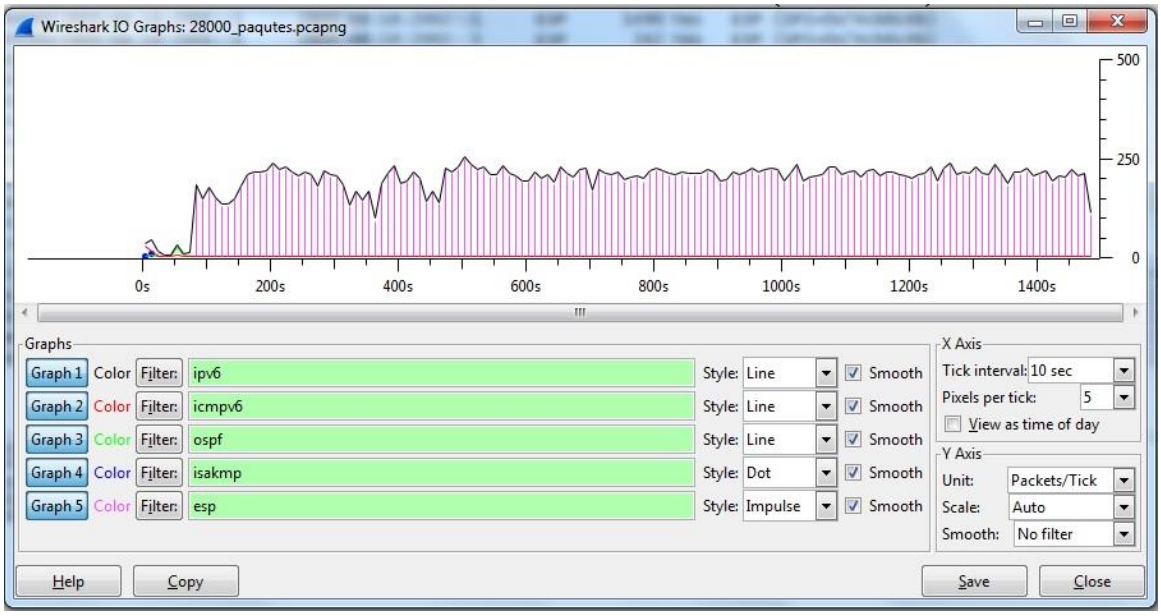
Estos resultados revelan que con la implementación del protocolo IPSec se duplica el número total de paquetes capturados a 28853, arrojando una diferencia de 14256 paquetes con referencia al escenario sin la implementación de IPSec con un total de 14597 paquetes. El aumento de paquetes se debe al aumento de cabeceras adicionales para la autenticación, la encriptación y como complemento para generar un canal seguro se crean paquetes o mensajes de autenticación con una clave compartida es decir la negociación del protocolo ISAKMP.

Como otro punto de comparación entre los dos escenarios de estudio, este análisis también se basa en el tiempo empleado en la trasmisión de paquetes de un extremo a otro, en virtud de la herramienta IO-Graphs de Wireshark con el cual es posible generar gráficas del comportamiento del tráfico de los protocolos durante un tiempo

determinado de muestreo sumado a la información proveniente de un resumen de la captura.

Se puede observar el comportamiento de la variación del tráfico durante el tiempo de muestreo, de hecho se puede observar el tiempo de transmisión de paquetes desde que se arrancan los dispositivos y el reconocimiento de la red hasta la finalización de ping extendido, se puede verificar en la figura 45, así como el tiempo empleado para realizar las negociaciones de los protocolos ISAKMP, OSPF y ICMPv6.

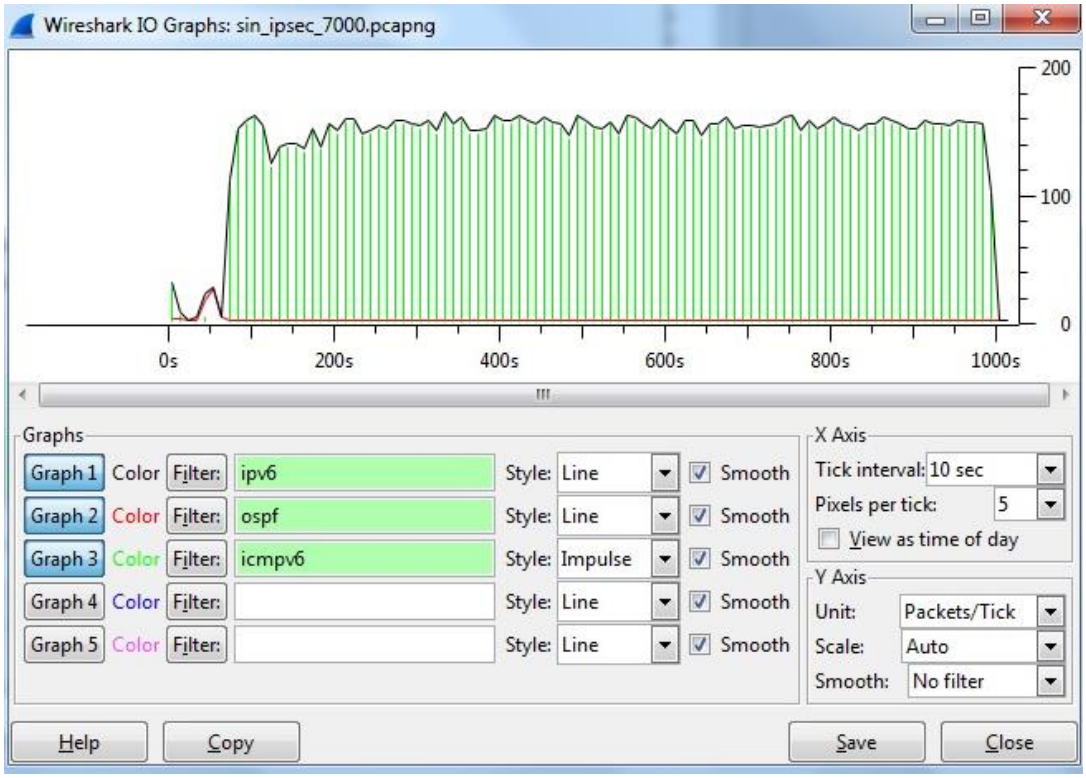
Figura 45 Variación del tráfico de los protocolos durante el tiempo de muestreo. Escenario con IPSec



Fuente: Captura del programa Wireshark

En el caso del escenario sin implementación de IPSec se puede interpretar que existe un menor tiempo de transmisión de los paquetes reflejados por el ping extendido sin embargo el tiempo de negociación de los protocolos OSPF e iCMPV6 son de manera similar al comportamiento del otro escenario de simulación. Tal comportamiento de verifica en la figura 46.

Figura 46 Variación del tráfico de los protocolos durante el tiempo de muestreo. Escenario sin IPSec



Fuente: Captura del programa Wireshark

De las evidencias anteriores, se tiene un valor aproximado del tiempo de retardo de los paquetes transmitidos desde el reconocimiento de la red hasta el fin del ping extendido, y mediante la captura de ping realizado en el escenario de simulación GNS3 se obtiene el tiempo promedio de transmisión por paquete obteniendo como resumen la tabla 10.

Tabla 10 Tabla de comparación de tiempo de retardo de los paquetes transmitidos

Escenario de Simulación	**Número de Paquetes Transmitidos**	**Tiempo de Retardo por paquete(ms) PING**	**Tiempo de retardo (s) entre el 1° y último paquete**
Implementado IPSec	28853	191	1488,852
Sin implementación de IPSec	14597	127	1019,119

Elaborado por: Berenice Arguero

Finalmente los resultados de análisis presentados anteriormente como: número de paquetes transmitido con su correspondiente porcentaje y el tiempo de retardo indican que con la implementación del protocolo se seguridad IPSec sobre el escenario de simulación entorno a la red avanzada de la UPS, se potenció la seguridad sobre esta red por la razón que se incrementó el número de paquetes transmitidos ya que estos son encriptados y encapsulados con tiempo promedio por paquete de 191 milisegundos, dando como resultado un incremento de 64 milisegundos por paquete; así mismo es relevante el aumento del tiempo de transmisión entre el primer paquete y el último paquete a 1488,852 segundos presentando una diferencia de 469,733 segundos a referencia del tiempo de transmisión del otro escenario de estudio que fue de 1019,119 segundos.

En cuanto a la diferencia anterior, el protocolo de seguridad implementado proporciona seguridad, sin embargo el tiempo de transmisión es un indicador que puede consumir de recursos de la red. Cabe considerar que la implementación se realizó con un solo túnel desde el router de frontera hasta el switch donde se encuentra elaborando las aplicaciones, y no se empleó varios túneles entre los dispositivos intermedio por motivo que hubiese reducido el desempeño de la red, potenciando así la seguridad en la red avanzada de la UPS y contribuyendo a que los prototipos o demos sean aplicados a la plataforma del Internet 2 sumado a esto también se beneficiaría la línea de investigación la Telemedicina, en el área de Telepediatría, el cual se encuentra asociado con el Centro de Salud N°3 La Tola en la Ciudad de Quito.

CONCLUSIONES

- Como resultado del análisis numérico presentado, se estableció que la implementación del protocolo IPSec es parte de la solución para brindar seguridad en la red avanzada de la UPS, con la finalidad que puedan ponerse en práctica los prototipos o demos que se encuentran desarrollando; esto se logró mediante la creación del túnel desde el router de frontera denominado Telconet hasta el switch denominado SUN el cual proporciona protección únicamente a los paquetes IP que se trasmiten por dicho canal dentro del escenario de estudio.

- Debe señalarse que la evaluación del comportamiento del protocolo de seguridad IPSec que se llevó a cabo, revela que hubo un incremento de alrededor del 50% con referencia a los paquetes dentro del escenario de estudio sin IPSec gracias a los resultados de los análisis numéricos. Es evidente que al implementar el protocolo ESP aumentaron el número de paquetes, empleando un 0,03% para la negociación y autenticación del túnel creado para posteriormente enviar los paquetes que se quiere proteger como la seguridad.

- Dentro del escenario de estudio con la implementación de IPSec se determinó que el tiempo empleado en la transmisión de los paquetes IP enviados de un extremo a otro en el escenario de simulación evidencian un aumento, esto se debe a que el proceso del encapsulamiento de cada paquete toma tiempo; la diferencia que hay entre un escenario respecto al otro es de 64 milisegundos por paquete, esto valida claramente que el implementar seguridades a nivel de capa red generará una sobrecarga en la red.

- El número de paquetes incrementados como el tiempo de transmisión son factores que se consideran importantes para la implementación del protocolo IPSec, es indudable que no se puede ignorar que estos factores reducen el desempeño de la red de Internet 2, pero pueden considerarse de menor degradación del desempeño mientras que esta red sea empleada para el desarrollo de la investigación y no como una red comercial.

- Este protocolo no fue implementado al resto de VLAN´s de la red de la UPS, por lo tanto es factible la implementación del protocolo IPSec como un método para brindar seguridad a la red de Internet 2 de la Universidad Politécnica Salesiana, Sede Quito Campus Sur.

RECOMENDACIONES

- Dentro de la infraestructura de la red de Internet 2 de la UPS se sugiere cambiar el switch 3COM de la serie 4200G de 24 puertos de 1Gbps al switch Catalyst 2960 de 48 puertos, puesto que el switch 3COM en sus características técnicas no soporta el protocolo IPSec.

- En el caso de la red avanzada de la UPS como estudio adicional, se deberá crear políticas de seguridad en torno a esta red para regularizar los procesos y gestión de la información con factores como: tiempo de vida de claves, creación de claves robustas, el control de acceso un sistema de detección de intrusos, etc.

- Proponer la integración de multicast sobre el protocolo de IPSec en la red de Internet 2 de la UPS; como complemento en la implementación se debería crear un servidor de claves y de usuarios de manera dinámica para dicha red.

- Una vez implementado el protocolo de seguridad IPSec en los respectivos segmentos seleccionados, se recomienda realizar periódicamente pruebas de seguridad orientadas a las aplicaciones que se están desarrollando actualmente sobre Internet 2.

- Realizar a futuro un análisis para implementar el protocolo de seguridad IPSec a toda la Universidad Politécnica Salesiana en la red del Internet 2, mientras que sea empleado a segmentos de red específicos por la razón que al emplear este protocolo se reduce el desempeño de la red.

LISTA DE REFERENCIAS

Alarcos, B., & De la Hoz, E. (2006). Recuperado el 10 de mayo de 2013, de http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t9-0506.pdf

Alarcos, B., & De la Hoz, E. (2006). Departamento de Automática. Recuperado el 19 de mayo de 2013, de http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t6-0506.pdf

Anónimo. (2005-2010). realidad virtual.com. Recuperado el 14 de enero de 2013, de Que es la realidad virtual: http://www.realidadvirtual.com/que-es-la-realidad-virtual.htm

Anónimo. (2008-2013). Definicion.de. Recuperado el 20 de julio de 2013, de http://definicion.de/ping/

Anónimo. (marzo de 2012). Recuperado el 18 de mayo de 2013, de http://networksafe.files.wordpress.com/2012/03/presentacion-hmac2.pdf

Anthony, B., & Steve, J. (Mayo de 2011). ciscopress.com. (I. Copyright © 2011 Pearson Education, Ed.) Recuperado el 25 de Mayo de 2013

Bruno, A., & Jordan, S. (mayo de 2011). ciscopress.com. (I. Copyright © 2011 Pearson Education, Ed.) Recuperado el 25 de mayo de 2013, de http://cisco.donntu.edu.ua/materials/640-864-ccda.pdf

Castro, E. (11 de junio de 2011). Recuperado el 28 de febrero de 2013, de http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

CEDIA. (26 de enero de 2010). IPv6. Recuperado el 28 de febrero de 2013, de http://ipv6.cedia.org.ec

CEDIA. (2012). IPV6.br. Recuperado el 15 de marzo de 2013, de http://ipv6.cedia.org.ec/elearning/ipv6_mod4.htm

CEDIA. (2012). Red Nacional de investigación y eduación del Ecuador. Recuperado el 23 de enero de 2013, de http://www.cedia.org.ec/index.php?option=com_content&view=article&id=1&Itemid=8

CISCO. (08 de julio de 2006). IP Routing. Recuperado el 19 de agosto de 2013, de Using the Extended ping and Extended traceroute Commands: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800 93f22.shtml#fielddesc

Cisco Systems, Inc. (31 de julio de 2012). Recuperado el agosto de 2013, de http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ipsec.pdf

Cisco Systems, Inc. (31 de julio de 2012). CISCO. Recuperado el 28 de julio de 2013, de Implementing IPsec in IPv6 Security: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ipsec.pdf

Corletti, A. (agosto de 2001). Worktec. Recuperado el 28 de abril de 2013, de http://www.worktec.com.ar/consetic2005/consecri/pdf/Consecri%2026-09-01/Sal%F3n%20General/Exposiciones/09-Protocolo%20IPSEC.pdf

GNS3. (28 de julio de 2009). GNS3 Graphical Network Simulation. Recuperado el 12 de julio de 2013, de http://iloo.wordpress.com/2009/07/28/gns3-simulador-grafico-de-redes/

Gonzalez, J. (abril de 2011). UCLA. Recuperado el 20 de marzo de 2013, de Repositorio : http://bibcyt.ucla.edu.ve/Edocs_bciucla/Repositorio/TGM_TK5105.585_G65_2011.pdf

González, L. (2011). Manual Oficial Virtual. Recuperado el 27 de junio de 2013, de RUANA: http://www.ruana.edu.co/procedimientos/Documents/Manual_Oficina_Virtual.pdf

INTECO-CERT. (junio de 2010). INTECO. Recuperado el 20 de marzo de 2013, de http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_implantacion_ipv6.pdf

LACNIC. (2012). Acerca de LACNIC. Recuperado el 20 de Julio de 2013, de http://www.lacnic.net/web/lacnic/acerca-lacnic

Manuel, H. J., & Ramón, M. (2002). Ramon Millan Articulos. (COIT & AEIT) Recuperado el 20 de febrero de 2013, de CONSULTORIA ESTRATEGICA EN TECNOLOGIA DE LA INFORMACION Y LA COMUNICACION: http://www.ramonmillan.com/tutoriales/mpls.php

Mendoza, M., & Carlos, C. (2002). CUDI. Recuperado el 30 de mayo de 2013, de Grupo de Seguridad: http://seguridad.cudi.edu.mx/grponly/congresos/ipsecfinal.pdf

Moreno, A., & Valencia, A. (marzo de 2012). Universidad Politécnica Salesiana Repositorio. Recuperado el 13 de julio de 2013, de http://dspace.ups.edu.ec/bitstream/123456789/3538/1/UPS-ST000848.pdf

ORACLE. (2010). Oracle. Recuperado el 11 de abril de 2013, de Guía de administración del sistema: servicios IP: http://docs.oracle.com/cd/E19957-01/820-2981/ipsec-ov-5/index.html

Pérez, S. (noviembre de 2001). Universidad Técnologica Nacional (Buenos Aires). Recuperado el 23 de abril de 2013, de http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

Perramon, X. (2008). Open Course Ware. Recuperado el 13 de mayo de 2013, de ocw.uoc.edu/computer-science...and.../P06_M2107_01772.pdf

Rallo, R., & Gisbert, M. (diciembre de 2002). Proyecto de Comunicación Avanzada TEL3D. Recuperado el 14 de enero de 2013, de http://www.sre.urv.es/web/tel3D/recursos/internet2.pdf

RedCLARA. (2012). Descripción Técnica. Recuperado el 20 de enero de 2013, de http://www.redclara.net/index.php?option=com_content&view=article&id=52&Itemid=423&lang=es

RedCLARA. (2012). NEG-Grupo de Ingenieria de la Red. Recuperado el 12 de marzo de 2013, de http://www.redclara.net/index.php?option=com_content&view=article&id=639&Itemid=500&lang=es

RedCLARA. (2012). Operaciones de la RedCLARA. Recuperado el 19 de enero de 2013, de http://www.redclara.net/index.php?option=com_content&view=article&id=18&Itemid=428&lang=es

RedCLARA. (2012). Servicios. Recuperado el 19 de enero de 2013, de http://www.redclara.net/index.php?option=com_content&view=article&id=861&Itemid=694&lang=es

Scientia et Technica Año XIV. (septiembre de 2008). Red de Revistas de America Latina y el Caribe , España y Portugal. Recuperado el 29 de mayo de 2013, de http://www.redalyc.org/articulo.oa?id=84920503057

Scott, H., & Eric, V. (2009). IPv6 Security. Recuperado el 9 de julio de 2013, de ciscopress.com: http://dark.ellende.eu/public/Cisco.Press.IPv6.Security.2009.pdf

Shirkar, A. (30 de mayo de 2013). CISCO SUPPORT COMUNITY, 9. Recuperado el 21 de agosto de 2013, de CISCO: https://supportforums.cisco.com/docs/DOC-27009#Topology_Diagram

The 6NET, Consortium. (octubre de 2005). Large-Scale International IPv6 Pilot Network. (M. Dumore, Ed.) Recuperado el 15 de marzo de 2013, de http://www.6net.org/book/deployment-guide.pdf

Universidad Católica de El Salvador. (junio de 2011). TICAL 2011. Recuperado el 27 de junio de 2013, de http://tical_2011.redclara.net/doc/Wilfredo_Bolanos.pdf

Universidad Politécnica Salesiana. (2011-2014). Investigacion. Recuperado el 23 de mayo de 2013, de http://www.ups.edu.ec/cima

UTPL. (2011). Proyectos de Investigación. Recuperado el 25 de febrero de 2013, de http://es.scribd.com/doc/93273628/2-introducciOn-a-la-telesalud-y-telemedicina

Yángüez, J. (noviembre de 2012). Unidad Docente de Sistemas (UDS). Recuperado el 20 de mayo de 2013, de http://www-lt.ls.fi.upm.es/scngn/images/documentacion/20122013/postgradoclase2-seguridad%20en%20ipv6-1noviembre2012.pptx.pdf

6SOS. (05 de enero de 2004). Documentos. (J. P. Martínez, Ed.) Recuperado el 25 de enero de 2013, de http://www.6sos.org/documentos/6SOS_Tutorial_IPv6_v4_0.pdf

Anexo 1 RFC's de IPv6

RFC	TÍTULO
RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
RFC2373	Arquitectura de Direccionamiento en IPv6
RFC2740	OSPF para IPv6
RFC2401	Arquitectura de Seguridad para IP
RFC2402	Cabecera de Autenticación IP
RFC2406	Encriptación de datos en IP (ESP)
RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)

Anexo 2 Configuración del Dispositivo Router Telconet

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RTelconet
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$K5Yo$ri4tuJWHXSkMSoGOns2cN0
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto keyring I2UPS
  pre-shared-key address ipv6 2800:68:16:2002::1/64 key hh87fkqwfw
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key ipsecvpn address ipv6 2800:68:16:2002::1/64
crypto isakmp profile 3des
   keyring I2UPS
   match identity address ipv6 2800:68:16:2002::1/64
!
crypto ipsec transform-set COMBINACION esp-3des esp-md5-hmac
!
```

```
crypto ipsec profile LISTA
 set transform-set COMBINACION
!
interface Loopback0
 no ip address
 ipv6 address 2800:68:16:2001::1/64
!
interface Loopback1
 no ip address
 ipv6 address FC00::1/64
!
interface Tunnel1
 no ip address
 ipv6 address 2800:68:16:2012::1/64
 ipv6 enable
 tunnel source 2800:68:16:2001::1
 tunnel destination 2800:68:16:2002::1
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile LISTA
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16::1/64
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 route FC01::/64 2800:68:16:2012::2
ipv6 route ::/0 FastEthernet0/0 2800:68:16::2
ipv6 router ospf 1
 router-id 10.1.1.1
 log-adjacency-changes
!
control-plane
!
banner motd AUTORIZADO
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
```

```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 logging synchronous
 login
End
```

Anexo 3 Configuración del Dispositivo Switch SUN

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SwSUN
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$x6iY$c16.uzUQvR0ZElIS56E5Z1
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto keyring I2UPS
  pre-shared-key address ipv6 2800:68:16:2001::1/64 key hh87fkqwfw
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key ipsecvpn address ipv6 2800:68:16:2001::1/64
crypto isakmp profile 3des
   keyring I2UPS
   match identity address ipv6 2800:68:16:2001::1/64
!
crypto ipsec transform-set COMBINACION esp-3des esp-md5-hmac
```

```
!
crypto ipsec profile LISTA
 set transform-set COMBINACION
!
interface Loopback0
 no ip address
 ipv6 address 2800:68:16:2002::1/64
!
interface Loopback1
 no ip address
 ipv6 address FC01::1/64
!
interface Tunnel1
 no ip address
 ipv6 address 2800:68:16:2012::2/64
 ipv6 enable
 tunnel source 2800:68:16:2002::1
 tunnel destination 2800:68:16:2001::1
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile LISTA
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16:600::2/64
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 route FC00::/64 2800:68:16:2012::1
ipv6 route ::/0 FastEthernet0/0 2800:68:16:600::1
!
control-plane
!
```

```
banner motd AUTORIZADO
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 logging synchronous
 login
end
```

Anexo 4 Configuración del Dispositivo Switch CORE

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SwCore
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$iUMp$DtVN52Cgk/EjpzEZX9rtM0
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16:1400::1/64
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16::2/64
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ipv6 route 2800:68:16:1000::/64 FastEthernet0/0 2800:68:16:1400::2
```

```
ipv6 route 2800:68:16:2001::/64 FastEthernet0/1 2800:68:16::1
ipv6 route 2800:68:16:2002::/64 FastEthernet0/0 2800:68:16:1400::2
!
control-plane
banner motd AUTORIZADO
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 logging synchronous
 login
end
```

Anexo 5 Configuración del Dispositivo Switch DISTRIBUCION

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SwDistribucion
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$mb6c$wzynSoXfN74rxobLB5TP1/
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16:1400::2/64
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16:1000::1/64
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ipv6 route 2800:68:16:600::/64 FastEthernet0/1 2800:68:16:1000::2
ipv6 route 2800:68:16:2001::/64 FastEthernet0/0 2800:68:16:1400::1
ipv6 route 2800:68:16:2002::/64 FastEthernet0/1 2800:68:16:1000::2
!
control-plane
banner motd AUTORIZADO
```

```
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 logging synchronous
 login
end
```

Anexo 6 Configuración del Dispositivo Switch ACCESO

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SwAcceso
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$duZV$jp.xiprAqODP5ASDQVDu1.
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16:1000::2/64
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2800:68:16:600::1/64
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ipv6 route 2800:68:16:1400::/64 FastEthernet0/0 2800:68:16:1000::1
ipv6 route 2800:68:16:2001::/64 FastEthernet0/0 2800:68:16:1000::1
ipv6 route 2800:68:16:2002::/64 FastEthernet0/1 2800:68:16:600::2
!
control-plane
```

```
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 logging synchronous
 login
!
!
```

GLOSARIO

Anti-replay: Es la protección contra la reproducción o duplicación de paquetes cifrados mediante la asignación de número de secuencia único para cada paquete cifrado.

IETF: (Internet Engineering Task Force) es una comunidad internacional cuyo objetivo es hacer que el Internet funcione mejor mediante la producción de documentos técnicos estandarizados para realizar el diseño y gestión del Internet.

IANA: (Internet Assigned Numbers Authority) es una identidad responsable de la coordinación mundial del direccionamiento IP, de los nombres de dominio y asignaciones de los protocolos.

LACNIC: (Latin America and Caribbean Network Infotmation Center), es una identidad no gubernamental que es el responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe (LACNIC, 2012)

Middleware: Es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogénea.

MTU: (Maximun Transmission Unit) es una característica de la capa enlace ya que indica el tamaño máximo de los paquetes de datos.

Ping: (Packet Internet Groper) es una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión. (Anónimo, 2008-2013)

Traceroute: Es una herramienta que descubre la ruta que realiza los paquetes de un punto hacia otro.

Clusters: Es un conjunto de computadoras independientes que forman parte de una arquitectura paralela distribuida que interconectados operan de una manera conjunta como un único recurso.