UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

(II Versión)

TEMA:

LOS PROTOCOLOS DE VoIP INCIDEN EN LA SEGURIDAD DE LA TRANSMISIÓN DE DATOS EN LA F.I.S.E.I. DE LA U.T.A. EN EL PRIMER SEMESTRE DEL AÑO 2010.

TESIS DE GRADO

Previa a la obtención del Título de Magíster en Redes y Telecomunicaciones

Nombre del Autor: Ing. Freddy Robalino Peña

Nombre del Director: Ing. Guevara David, M.Sc

Ambato - Ecuador

2011

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, nombrado por el H. Consejo de Postgrado de la Universidad Técnica de Ambato

CERTIFICO:

Que el Informe de Investigación: "Los protocolos de VoIP inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A. en el primer semestre del año 2010.", presentada por el maestrante: Ing. Edgar Freddy Robalino Peña, estudiante del programa de Maestría en Redes y Telecomunicaciones (II Versión), reúne los requisitos y méritos suficientes para ser sometido a la evaluación del jurado examinador que el H. Consejo de Posgrado designe.

Ambato, 14 de Enero del 2011.

TUTOR

_____

Ing. Guevara David, M.Sc.
C.I: 1802605749

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de investigación con el tema "**LOS PROTOCOLOS DE VoIP INCIDEN EN LA SEGURIDAD DE LA TRANSMISIÓN DE DATOS EN LA F.I.S.E.I. DE LA U.T.A. EN EL PRIMER SEMESTRE DEL AÑO 2010.**" , nos corresponde exclusivamente a Edgar Freddy Robalino Peña, Autor y David Omar Guevara Aulestia, Director de la Tesis de Grado; y el patrimonio intelectual de la misma a la Universidad Técnica de Ambato.

Ambato, 14 de Enero del 2011

_____	_____
Ing .Freddy Robalino P	Ing. Guevara David, M.Sc.
C.I. 1803299351	C.I: 1802605749
Autor	Director de Tesis

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de esta tesis o parte de ella un documento disponible para su lectura, consulta y procesos de investigación, según normas de la Institución.

Cedo los Derechos en línea patrimoniales de mi tesis, con fines de difusión pública, además apruebo la reproducción de esta tesis, dentro de las regulaciones de Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Ambato, 14 de Enero del 2011

_____

Ing .Edgar Freddy Robalino Peña

Al consejo de posgrado de la UTA

El comité de defensa de Tesis de Grado. "**LOS PROTOCOLOS DE VoIP INCIDEN EN LA SEGURIDAD DE LA TRANSMISIÓN DE DATOS EN LA F.I.S.E.I. DE LA U.T.A. EN EL PRIMER SEMESTRE DEL AÑO 2010.**" presentada por: Ing .Freddy Robalino P y Conformada por: Ing. Clay Aldás M.Sc Ing. Teresa Freire M.Sc, Ing. Galo López M.Sc, Miembros del Tribunal de Defensa, Ing. Guevara David, M.Sc, Director de Tesis de Grado y presidido por: Ing. Oswaldo Paredes, M.Sc, Decano; Director del CEPOS-UTA, Ing. M.Sc. Luis Velásquez Medina, una vez escuchada la defensa oral y revisada la Tesis de Grado escrita en la cual se ha constatado el cumplimiento de las observaciones realizadas por el Tribunal de Defensa de la Tesis, remite la presente Tesis para uso y custodia en la biblioteca de la UTA.

_____ _____

Ing. Oswaldo Paredes, M.Sc
Presidente del Tribunal de Defensa

Ing. M.Sc. Luis Velásquez Medina
DIRECTOR DEL CEPOS

_____

Ing. Guevara David, M.Sc
Director de Tesis

_____

Ing. Clay Aldás, M.Sc
Miembro del Tribunal

_____

Ing. Teresa Freire, M.Sc
Director de Tesis

_____

Ing. Galo López, M.Sc
Director de Tesis

DEDICATORIA

Dedico este proyecto y toda mi carrera a Dios por ser quien ha estado a mi lado en todo momento dándome las fuerzas necesarias para continuar luchando día tras día y seguir adelante superando todas las barreras que se me presenten.

A mi amada esposa Gissela que con paciencia y ternura ha sabido ser una verdadera compañera en este momento importante de mi vida, a mis hijos Alan Mateo y Michelle Alexandra por ser el motivo y la razón de mi esfuerzo y dedicación, a mis queridos padres Amado y María Gloria que me han apoyado y acompañado todos y cada uno de los momentos de mi vida, a mis adoradas hermanas por compartir mis alegrías y alentarme a seguir en el camino de la superación.

A mi noble y tan importante hermano Christian Andrés que es como un hijo más para mí, y que aunque no estemos siempre juntos este esfuerzo también se lo dedico a él, como ejemplo de decisión y superación.

Freddy Robalino

AGRADECIMIENTO

Quiero expresar mis más sinceros agradecimientos a todas las personas que contribuyeron a la culminación de este proyecto, en especial al Ingeniero David Guevara, por su calidad humana, conocimiento, y muy acertada dirección.

No puedo dejar pasar por alto y expresar mi agradecimiento al Ing. Oswaldo Paredes en calidad de Decano y Presidente de Postgrado, por la experiencia y conocimientos brindados en el diseño de este proyecto, pero sobre todo por el apoyo y empuje que ha sabido darnos a todos los nosotros en calidad de maestrantes ya que sin su trabajo desinteresado, no hubiésemos encontrado la meta final.

Un agradecimiento especial a la Universidad Técnica de Ambato y a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial por brindarme la oportunidad a través de ésta maestría de ampliar mis conocimientos en el área de las Redes y Telecomunicaciones.

Freddy Robalino

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

La investigación sobre "Los protocolos de VoIP inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A. en el primer semestre del año 2010", tiene como objetivo general reflexionar sobre, nivel de seguridad en la transmisión de datos (VoIP) que proporcionan los protocolos adyacentes a esta tecnología. En la actualidad podemos encontrar mucha información sobre la transferencia de la voz sobre IP (VoIP) y de cómo implementar esta tecnología, pero poca información de cómo lograr que estas trasmisiones sean seguras o de cómo se podría mejorar su calidad. El énfasis se centra en la selección del mejor protocolo que incremente la seguridad en la transmisión de Voz sobre IP.

Este tema enfrenta este problema analizando los protocolos más comunes en la transmisión de voz sobre IP: el protocolo H.323[1] y SIP[2], comparando su rendimiento y nivel de seguridad que ofrece cada uno de ellos. De esta manera se presentan los criterios básicos sobre una transferencia de voz sobre IP segura.

DESCRIPTORES: Seguridad en la transmisión de datos, Protocolos VoIP, H.323, SIP, códecs, Red LAN.

INTRODUCCIÓN

En el transcurso de la historia, las innovaciones técnicas han llevado con frecuencia a cambios significativos en las comunicaciones interpersonales, con influencia significativa en toda la sociedad.

En los últimos años, ha ido ganando fuerza un nuevo tipo de tecnología de comunicación: las redes interactivas, que permiten a los usuarios enviar o recibir una gran cantidad de información. La red interactiva de más rápido crecimiento y la más grande hasta el momento ha sido Internet. Reservado, hasta hace pocos años, a los científicos y a los fanáticos de la tecnología, su número de usuarios ha crecido dramáticamente en un tiempo muy corto, gracias a las facilidades de acceso, a la disponibilidad de ordenadores potentes a un coste asumible y, sobre todo, al carácter cada vez más informativo y de entretenimiento de esa Red de Redes.

Mientras, la disponibilidad de conexiones de banda ancha a Internet ha crecido igualmente rápido, lo que nos sitúa en el umbral de una innovación revolucionaria la voz y la telefonía sobre Internet, combinará los antiguos y nuevos métodos de comunicación el cual tendrá, de nuevo, un fuerte impacto social. Ningún mercado ha crecido tan rápidamente, ni ha tenido tanta publicidad, como el de la Voz sobre IP. Mientras el principal interés de los usuarios privados se centra en cómo reducir sus facturas de teléfono, las ventajas en términos de costos para las empresas están relacionadas sobre todo con las sinergias que se conseguirán con esta tecnología, al consolidar las telecomunicaciones existentes y la infraestructura TI^3 dentro de Ethernet, pero existen riesgos en el entorno VoIP.

A pesar de la euforia con esta tecnología, que supondrá una burbuja de aire para el complejo y enfrentado mundo de las TI^3 y las telecomunicaciones, debemos ser conscientes de que la telefonía y la voz sobre el Internet es vulnerable y están expuestas a los mismos riesgos que afrontan diariamente los usuarios IP. Es por ello que la seguridad en el ámbito VoIP tiene una importancia clave. La misma,

sin embargo, hoy por hoy, no ocupa el lugar que le corresponde en la mente del usuario, más preocupado por garantizar la capacidad de comunicarse a través de esa tecnología.

La importancia de la seguridad en la transmisión de Voz sobre IP, sobre todo para las comunicaciones de negocio, ha quedado demostrada por numerosos estudios, entre ellos, por la reciente publicación de la (BSI[4]).

Descripción de Capítulos que conforman la investigación

El CAPÍTULO I - EL PROBLEMA contiene:

El planteamiento del problema, su contextualización, interrogantes, justificación y objetivos con el fin de clarificar el contexto sobre el cual se va a desarrollar la investigación de los protocolos y seguridades de VoIP utilizados en la F.I.S.E.I.

El CAPÍTULO II - MARCO TEÓRICO contiene:

La base teórica sobre las tecnologías, protocolos VoIP utilizados en la red de datos, y los métodos de seguridad que se dan a la transmisión de voz, determinando la arquitectura actual, sus componentes, y la posible implementación de seguridades.

El CAPÍTULO III - METODOLOGÍA contiene:

La metodología, el tipo de investigación y recolección de información, que será usada en el análisis de datos, verificación de hipótesis, con un análisis de características, parámetros técnicos de los diferentes protocolos, las seguridades implementadas y como están adaptados a la red, además se indica los resultados obtenidos y propuestas de nuevas líneas de investigación para futuros trabajos.

El CAPÍTULO IV - ANÁLISIS E INTERPRETACIÓN DE RESULTADOS Contiene:

La descripción de la situación actual y diagnóstico, con un análisis de la red existente y la red de datos, tanto como los protocolos implementados que aseguren la transmisión de VoIP.

El CAPÍTULO V – CONCUSIONES Y RECOMENDACIONES contiene:

Las conclusiones y recomendaciones a los objetivos planteados del trabajo realizado.

El CAPÍTULO VI - LA PROPUESTA contiene:

La viabilidad técnico económico del proyecto en base a la tecnología implantada, cambio de políticas de seguridad y beneficio para la facultad a través de la selección del o los protocolos que incrementen el nivel de seguridad en las transmisiones a través de una red VPN con IPSec.

CAPÍTULO I

El Problema

Planteamiento del Problema

"Tema: LOS PROTOCOLOS DE VoIP INCIDEN EN LA SEGURIDAD DE LA TRANSMISIÓN DE DATOS EN LA F.I.S.E.I. DE LA U.T.A. EN EL PRIMER SEMESTRE DEL AÑO 2010"

Contextualización

Macro

Según el artículo publicado por la Unión Internacional de Telecomunicaciones Publicado el 01 de Mayo del 2010.- En todo el mundo, los operadores telefónicos locales y de larga distancia, las empresas de televisión por cable, los proveedores de servicios Internet, los proveedores independientes sin infraestructura y los operadores móviles ofrecen servicios telefónicos por protocolo Internet (VoIP). El número de abonados a esta tecnología y los ingresos que genera están aumentando considerablemente.

Todas estas tecnologías entrañan la digitalización, conversión y compresión de señales de voz en paquetes de datos que se transmiten por una red IP y que se vuelven a ensamblar y convertir en señales vocales en el extremo receptor.

Los principales factores que propician la adopción y generalización de la VoIP son, entre otros para las empresas y sus usuarios la seguridad por un coste inferior: Para los usuarios institucionales y comerciales, una red privada es más rentable, segura y fiable, sin pérdida apreciable de la calidad de servicio.

Para los consumidores, precios más bajos y facturación más sencilla, el crecimiento explosivo de empresas tales como Skype[5] y Vonage[6] demuestra la influencia del poder de la demanda de los consumidores en el crecimiento de la VoIP.

Esta tecnología también puede reducir los obstáculos a la entrada en nuevos mercados geográfico. Los ingresos generados por la VoIP podrían compensar la disminución de los generados por la telefonía tradicional y permitir que los operadores entren en el creciente mercado de la banda ancha.

Innovación mejorada: Es relativamente fácil añadir medios a comunicaciones basadas en el IP. También pueden ofrecerse nuevos servicios por una red IP convergente y algunos pueden añadirse a través de interfaces con equipos RTPC existentes.

Nuevos modelos de actividad comercial: La VoIP ofrece la posibilidad de adoptar nuevos modelos de actividad comercial tales como la tarifa plana, u obviar el tradicional sistema de liquidación de tasas de distribución.

En algunos mercados, sin embargo, la VoIP parece no alcanzar su pleno potencial. Los obstáculos al crecimiento son, entre otros los problemas de QoS y fiabilidad: Los servicios de voz, vídeo y datos de alta velocidad tienen necesidades diferentes y, por lo tanto, los servicios agrupados imponen exigencias diferentes a las redes en materia de calidad de servicio (QoS). La capacidad de la red para funcionar a pesar de los cortes de corriente es un problema que aqueja particularmente a los países en desarrollo. En cuanto a la seguridad, en VoIP sólo puede obtenerse información limitada sobre la parte llamante.

Los operadores establecidos pueden considerar que la VoIP es una amenaza para sus ingresos generados por la RTPC (Redes telefónicas públicas), principalmente en países en los cuales el mercado es monopolístico o carece de madurez.

Los operadores aducen que, para justificar grandes inversiones en redes de banda ancha para la VoIP, necesitan un marco normativo claro y predecible que les ayude a garantizar la rentabilidad de sus inversiones.

Algunos países están elaborando normativas para la VoIP (por ejemplo, obligaciones de llamadas de emergencia) que podría dificultar la entrada de nuevos actores que desean ofrecer servicios VoIP.

Meso

Según la publicación hecha, el 14 de abril de 2009.- WatchGuard® Technologies, proveedor global de soluciones de seguridad de red y su filial en el ecuador, ha elaborado un listado con las principales amenazas para la seguridad de la Voz sobre IP (VoIP), dado que se ha convertido en uno de los objetivos de los ciber-criminales ante su fuerte crecimiento.

De acuerdo con los últimos informes publicados se predice que alrededor del 55% de las líneas de teléfono corporativas en el Ecuador utilizarán VoIP en los próximos dos años, mientras que se espera que la mitad de las pymes y dos tercios de todas las organizaciones ecuatorianas utilicen VoIP. Asimismo, se espera que a final de año el número total de usuarios de VoIP, tanto residenciales como comerciales, llegue a los 10000 usuarios en el país.

Debido a la ubicuidad de la VoIP, ésta alternativa se está convirtiendo rápidamente en un nuevo vector de amenazas para las empresas de todo el mundo y de sobre manera en nuestro país debido a que no existen reglamentación ni políticas de seguridad expedidas por el por los entes reguladores solo existen de funcionamiento.

“Así como las redes de datos en los países latinoamericanos han sucumbido a las amenazas, los sistemas de voz sobre IP se enfrentan a una ruta paralela ", ha señalado Eric arrestad, Vicepresidente de WatchGuard Technologies. "A medida

que las organizaciones continúen con los procesos de convergencia de redes y sigan adoptando la tecnología VoIP, tanto las grandes empresas como las de menor tamaño tendrán que evolucionar y desarrollar su arquitectura de seguridad (protocolos) para garantizar que sus clientes, los usuarios y la transmisión de datos están a salvo de las amenazas de VoIP".

Micro

La investigación actual contempla el tipo de protección en la transmisión de los datos y los protocolos VoIP de seguridad implementados en la red de la F.I.S.E.I. además del estudio de la vulnerabilidad de la red debido a no implementación de arquitecturas de seguridad apropiados que den confiabilidad al usuario.

Aun cuando el sistema operativo, pueden escanear rangos de direcciones IP enteros de forma aleatoria y oculta, e incluso enviar "escaneos señuelo" para hacer más difícil al objetivo el identificar quien es realmente el origen de la agresión.

Los atacantes también intentan atacar a los sistemas de detección de intrusos, ya sea saturándolos de tráfico a analizar o bien mediante herramientas que les proporcionan información falsa de lo que pasa por la red. El hecho de que los atacantes estén incorporando técnicas anti-IDS[8] a su arsenal, los coloca en situación más ventajosa frente a organizaciones que ni siquiera disponen de un IDS, aun peor carecen del conocimiento para una buena selección de protocolos que eviten las intrusiones internas y externas a la red.

Árbol de Problemas

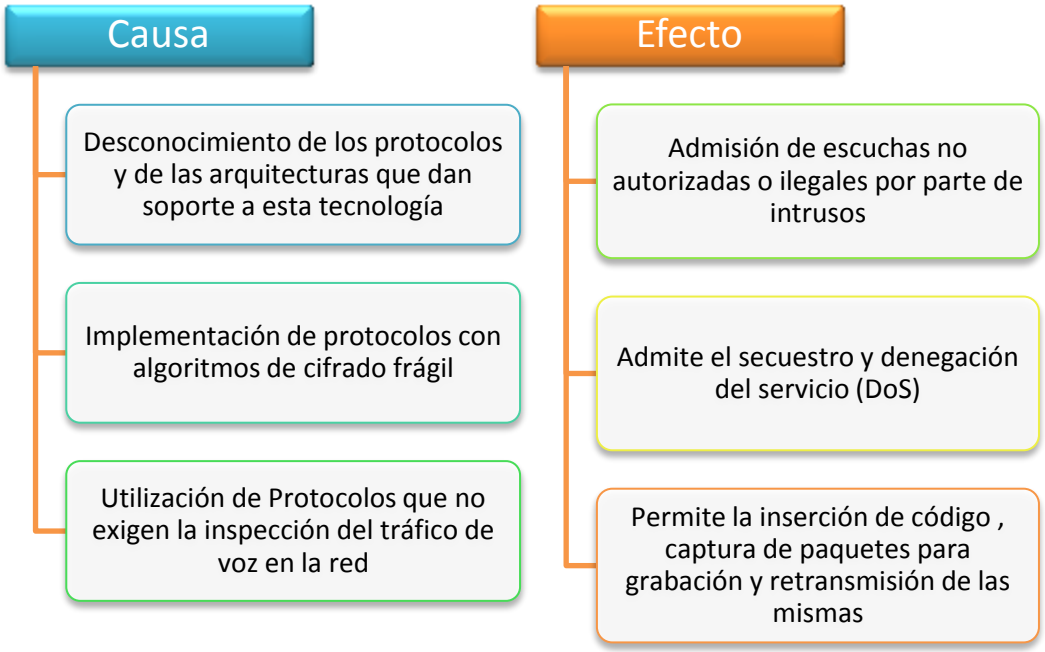


Figura No. 1.1: Relación Causa – Efecto
Elaborado por: Freddy Robalino

Análisis Crítico

La inseguridad en los protocolos de transmisión de VoIP en la red es uno de los problemas propios de la tecnología y los sistemas de protección puestas en esta. Como muchas de las nuevas tecnologías presentan situaciones favorables, esta también tiene riesgos e inconvenientes.

La privacidad es una gran preocupación para las corporaciones e instituciones como la nuestra que implementan VoIP. La privacidad de la señalización y las llamadas es extremadamente importante. Una señalización expuesta, debido a la poca seguridad en la transmisión puede proporcionar información a espías sobre los patrones de las llamadas: cuando se realizan, quien participa en la llamada, longitud de tiempo que permaneció activa, que protocolos seguridad se utilizan, las arquitecturas etc.

Dependiendo de las circunstancias, el simple conocimiento de la existencia de una llamada puede proporcionar información a un extraño que desemboque en consecuencias negativas, como la denegación de los servicios, esto por la falta de conocimiento para la implantación de estándares que protejan eficientemente los datos y aún más la voz. Por otra parte, los paquetes de las conversaciones de voz no encriptados, pueden ser capturados y posteriormente re- ensamblados en archivos audibles de tipo '.WAV[9]' utilizando herramientas disponibles gratuitamente en Internet, para luego ser montadas y retransmitidas en la red.

Comúnmente, los administradores de redes cometen el error de pensar de que al momento de digitalizar la voz y que ésta viaje en paquetes a través de sus instalaciones de red "segura", esta le será transferida a la voz, dicha seguridad de la red IP, tecnología donde por naturaleza se comparte el medio.

Para el buen funcionamiento del servicio VoIP, es necesario reforzar la seguridad de la digitalización de la voz, de manera independiente de la establecida en la red, dando un tratamiento preferencial a ciertos protocolos o nodos dentro de ella.

El hecho de que la voz esté en un medio compartido que comunica servicios y/o recursos, base del diseño del protocolo IP que no se hizo para brindar seguridad por sí misma, resulta problemático ofrecer las bases de la seguridad que son: confidencialidad, integridad, autenticidad y disponibilidad.

Es fundamental hacer mejoras y el permanecer siempre alerta y vigilante en las redes de voz, poniendo especial atención y procurando implementar protocolos con algoritmos de cifrado alto que exijan inspección del tráfico de voz, para esto se necesitara, capacitaciones e investigaciones para luego poder escoger las mejores alternativas.

Prognosis

En la actualidad existen protocolos que tienen seguridades pero por desconocimiento de su funcionamiento y sus algoritmos de compresión, no son utilizados, además las vulnerabilidades en los equipos y servicios que permiten esta tecnología necesitan ser descubiertos y mitigados", si no se pone énfasis en el políticas de seguridad implementadas en la institución como el uso de estándares seguros traerá una serie de problemas, como la captura de información, inseguridad en la trasmisión y desconfianza de los usuarios en el uso de esta tecnología

Formulación del Problema

¿Cómo inciden los protocolos de VoIP en la seguridad de la transmisión de datos en la red?

Preguntas Directrices

- ¿Cuáles son los protocolos de VoIP que se utilizan en la red de la F.I.S.E.I.?
- ¿Cuál es el nivel de seguridad en transmisión de datos?

- ¿Existen alternativas de solución a la inseguridad que ofrecen los protocolos de VoIP para la transmisión de datos?

Delimitación de la Investigación

Campo: TELECOMUNICACIONES

Área: REDES LAN

Aspecto: PROTOCOLOS DE VOIP Y SEGURIDAD EN LA TRANSMISIÓN DE DATOS.

Delimitación Espacial:

La investigación se la realizó en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, donde se recolectó información necesaria, la misma que será utilizada en el análisis de la propuesta, así como el uso de información bibliotecaria para fundamentar el uso y empleo de los estándares y protocolos de estudio

Delimitación Temporal:

El desarrollo de la investigación se la efectuó en el primer semestre del año 2010.

Unidades de Observación:

- Administración de Redes
- Ayudantes de Laboratorio
- Centro de Transferencia de Tecnologías (C.T.T.)
- UOCENIC

Justificación

La VoIP permite la unión de dos mundos históricamente separados, el de la transmisión de voz y el de la transmisión de datos. Entonces, el VoIP no es un servicio sino una tecnología. VoIP puede transformar una conexión estándar a internet en una plataforma para realizar llamadas gratuitas por internet. Usando algunos de los software gratuitos para llamadas VoIP que están disponibles en internet estamos dejando de lado a las compañías tradicionales de telefonía, y por consiguiente, sus tarifas.

En el pasado, las conversaciones mediante VoIP solían ser de baja calidad, esto se vio superado por la tecnología actual y la proliferación de conexiones de banda ancha, hasta tal punto llego la expansión de la telefonía ip que existe la posibilidad de que usted sin saberlo ya haya utilizado un servicio VoIP, por ejemplo, las operadoras de telefonía convencional, utilizan los servicios del VoIP para transmitir llamadas de larga distancia y de esta forma reducir costos.

Se sabe que va a llevar algún tiempo pero es seguro que en un futuro cercano desaparecerán por completo las líneas de teléfono convencionales que utilizamos en nuestra vida cotidiana, el avance tecnológico indica que estas serán muy probablemente reemplazadas por la telefonía IP.*Por DarringMulligan, Vicepresidente de eLoyaltyCorporation.*

Pero hay un factor preponderante "La Seguridad en la transmisión de voz sobre ip" esta es muy necesaria e indispensable, que casi en los 17 años creación, desarrollo y evolución de este tipo de tecnología y forma de comunicación está formando parte de la vida cotidiana de un número cada vez mayor de personas, la cual nos está sorprendiendo, interesando e inspirando. Este nuevo medio de comunicación está seduciendo a millones por las posibilidades y alcances de un mundo donde personas de todo tipo de ideas y culturas, con variadas y extremas obsesiones conviven, se conocen, comunican y hasta hacen negocios en un marco de libertad imposible para otros medios de comunicación.

Sin embargo, la inseguridad llega a espantar a muchos y diversas voces alertan sobre el uso de la tecnología por las mafias, personas conocidas como VoIP hackers, VoIP phishing [10], y los Spam VoIP. La falta de reglamentación y el uso de protocolos del cual no conocemos que hacen y como trabajan, han generado dudas sobre si es seguro o no transmitir y aun peor hacer sesiones ya de tipo comerciales utilizando este medio y este tipo de tecnología de comunicación, muchos padecen el miedo, real o imaginario, de que personas o programas sofisticados puedan vulnerar los protocolos de transmisión y violar la privacia de los usuarios o internarse incógnitos tomar el control, la información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y dirigir llamadas, un atacante puede obtener un mapa detallado de todas las llamadas realizadas en tu red, creando grabaciones completas de conversaciones y datos de usuario.- Se teme, también, por la educación, los valores de los niños y adolescentes que, destacan entusiastas como posibles usuarios de esta forma de comunicación.

Estas consideraciones han sido recogidas por empresas desarrolladoras de equipos, software y protocolos de seguridad, las cuáles han puesto en el mercado protocolos no muy seguros para calmar los nervios de quienes encuentran utilizando esta tecnología.

Si se pone énfasis en las políticas de seguridad y se implantan protocolos con alta seguridad, los usuarios de esta tecnología van a experimentar varios cambios con una solución IP segura, así incrementara la confianza, uso, y la masificación del mismo.

Objetivos

Objetivo General

Determinar la incidencia de los Protocolos de VoIP en la seguridad de la transmisión de datos en la red de la F.I.S.E.I. de la U.T.A. en el primer semestre del año 2010.

Objetivos Específicos:

- Determinar cuáles son los protocolos de VoIP utilizados en la F.I.S.E.I.
- Cuantificar el nivel de seguridad en Transmisión de datos
- Analizar la mejor alternativa de solución, mediante la selección de la principal herramienta de análisis y simulación de red.

CAPITULO II

Marco Teórico

Antecedentes de Investigación

En la investigación previa se ha encontrado esta tesis relacionada con seguridad y protocolos VoIP:

Galo Iturralde Orellana y Cristina Abad Robalino estudiantes de la FIEC carrera Ingeniería en Computación Science, 2003 (University of Illinois); Estudio de Seguridades VoIP y Desempeño de los Protocolos en Redes con Clientes Inalámbricos.

"Actualmente podemos encontrar variedad de información sobre cómo implementar voz sobre IP (VoIP), pero muy poca información con respecto a cómo lograr que estas trasmisiones sean seguras o de cómo se podría mejorar su calidad. El énfasis se centra generalmente en como logramos una transmisión segura."

Se ha investigado en las bibliotecas de las Universidades de Ambato y no se ha encontrado tesis específicas al tema propuesto.

Fundamentaciones

Fundamentación Legal

Debido a que el estudio se refiere al campo de las telecomunicaciones es necesario especificar las leyes referentes a los protocolos de transmisión de datos y los estándares de seguridad establecidas por los organismos internacionales como la (UIT) Unión Internacional de Telecomunicaciones y (IETF) Internet EngineeringTask Force - Grupo de Trabajo en Ingeniería de Internet.

REGLAMENTO GENERAL A LA LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA

ALCANCE Y DEFINICIONES

Artículo 1. El presente reglamento tiene como finalidad establecer las normas y procedimientos generales aplicables a las funciones de planificación, regulación, gestión y control de la prestación de servicios de telecomunicaciones y la operación, instalación y explotación de toda transmisión, emisión o recepción de signos, señales, imágenes, datos y sonidos por cualquier medio; y el uso del espectro radioeléctrico.

Artículo 2. Las definiciones de los términos técnicos de telecomunicaciones serán las establecidas por la Unión Internacional de Telecomunicaciones - UIT, la Comunidad Andina de Naciones - CAN, la Ley Especial de Telecomunicaciones y sus reformas y este reglamento.

DEL RÉGIMEN DE LOS SERVICIOS

Artículo 5. Para la prestación de un servicio de telecomunicaciones, se requiere un título habilitante, que habilite específicamente la ejecución de la actividad que realice.

Artículo 7. Son servicios portadores aquellos que proporcionan a terceros la capacidad necesaria para la transmisión de signos, señales, datos, imágenes y sonidos entre puntos de terminación de una red definida, usando uno o más segmentos de una red. Estos servicios pueden ser suministrados a través de redes públicas conmutadas o no conmutadas integradas por medios físicos, ópticos y electromagnéticos.

RESOLUCIÓN 491-21-CONATEL-2006
CONSEJO NACIONAL DE TELECOMUNICACIONES
CONATEL

CONSIDERANDO:

Que de conformidad a la Ley Especial de Telecomunicaciones y sus reformas y al Reglamento General a la Ley Especial de Telecomunicaciones Reformada, el CONATEL es el ente público encargado de establecer, en representación del Estado, las políticas y normas de regulación de las telecomunicaciones en el Ecuador.

Que el avance tecnológico ha impulsado la introducción de programas y aplicaciones sobre la red Internet, que facilitan la transmisión y recepción de voz, video y datos.

Que los proveedores de Servicios de Valor Agregado de Internet están facultados legalmente por el CONATEL para la provisión de acceso a Internet.

Que los Centros de Acceso a Internet y Ciber Cafés están regulados mediante la Resolución 073-02-CONATEL-2005, demás normas y regulación vigente.

Que Internet, por su naturaleza de red global, opera sobre una infraestructura distinta de las redes públicas de telecomunicaciones que se han desplegado dentro de territorio ecuatoriano, de conformidad con la legislación y normativa vigente.

Que la denominada Voz sobre IP, identificada con las siglas VoIP, es un término genérico que incluye varias modalidades de uso que requieren ser diferenciadas para determinar la aplicación de normas de regulación y control vigentes dentro del territorio del Ecuador.

Que el denominado Protocolo de Internet, identificado por las siglas IP, es un lenguaje de transmisión de información caracterizado por el envío de datos en formato de paquetes.
En ejercicio de sus facultades,

RESUELVE:

ARTÍCULO UNO. La Voz sobre Internet, cursada a través de la red Internet, permite a sus usuarios comunicarse entre sí o entre un usuario conectado a la red Internet con un usuario conectado a una Red Pública de Telecomunicaciones. La Voz sobre Internet es reconocida como una aplicación tecnológica disponible en Internet. El video, los datos y multimedios cursados a través de la red Internet, son igualmente reconocidos como aplicaciones tecnológicas disponibles en Internet.

ARTÍCULO DOS. Cuando un operador de telecomunicaciones preste el servicio de telefonía utilizando Protocolo IP, el operador está sujeto al marco legal, las normas de regulación y control aplicables. **RESOLUCIÓN 491-21-CONATEL-2006 2**

ARTÍCULO TRES. Los proveedores de Servicio de Valor Agregado de Internet no restringirán a sus usuarios el acceso a las aplicaciones detalladas en el Artículo 1 de la presente Resolución, incluido su uso, sin perjuicio de origen, marca o proveedor de tales aplicaciones.

ARTICULO CUATRO. Cualquier persona natural o jurídica, incluyendo a los proveedores de Servicio de Valor Agregado de Internet dentro de los servicios que prestan a sus usuarios, podrán comercializar dispositivos y planes para el uso de las aplicaciones detalladas en el Artículo 1 de la presente Resolución.

ARTICULO CINCO. Ninguna persona natural o jurídica, incluyendo a los Proveedores de Servicio de Valor Agregado de Internet, podrán usar, dentro del territorio nacional, dispositivos de conmutación, tales como interfaces o

compuertas (Gateways) o similares, que permitan conectar las comunicaciones de Voz sobre Internet o las llamadas sobre Internet a las Redes Públicas de Telecomunicaciones del Ecuador.

Se exceptúan de esta limitación a los operadores de telecomunicaciones debidamente autorizados.

ARTICULO SEIS. El CONATEL, a través de la SENATEL, no concederá recurso de numeración telefónica, de conformidad al Plan Técnico Fundamental de Numeración, para las aplicaciones detalladas en el Artículo 1 de la presente Resolución.

ARTÍCULO OCHO. Sustitúyase el literal d) del Artículo tres (3) de la Resolución 073-02-CONATEL-2005 por el siguiente: literal "d) Los "Centros de información y acceso a la red de Internet" o "Ciber Cafés" que ofrezcan voz sobre Internet, de conformidad con lo señalado en el literal a) del presente artículo requerirán únicamente de un certificado de registro, de conformidad con el artículo 7 de la presente resolución;".

ARTÍCULO NUEVE. Encárguese a la SENATEL que, en el término de noventa días, elabore los parámetros de calidad, las consideraciones de numeración, interconexión y otros aspectos necesarios para los operadores legalmente autorizados que brinden Telefonía sobre Protocolo IP.

La presente Resolución es de ejecución inmediata y entrará en vigencia a partir de la presente fecha, sin perjuicio de su publicación en el Registro Oficial.

Dado en Quito, 8 de septiembre de 2006.

Dr. Juan Carlos Solines Moreno

Presidente del Conatel

Ab. Ana María Hidalgo Concha

Secretaria del Conatel

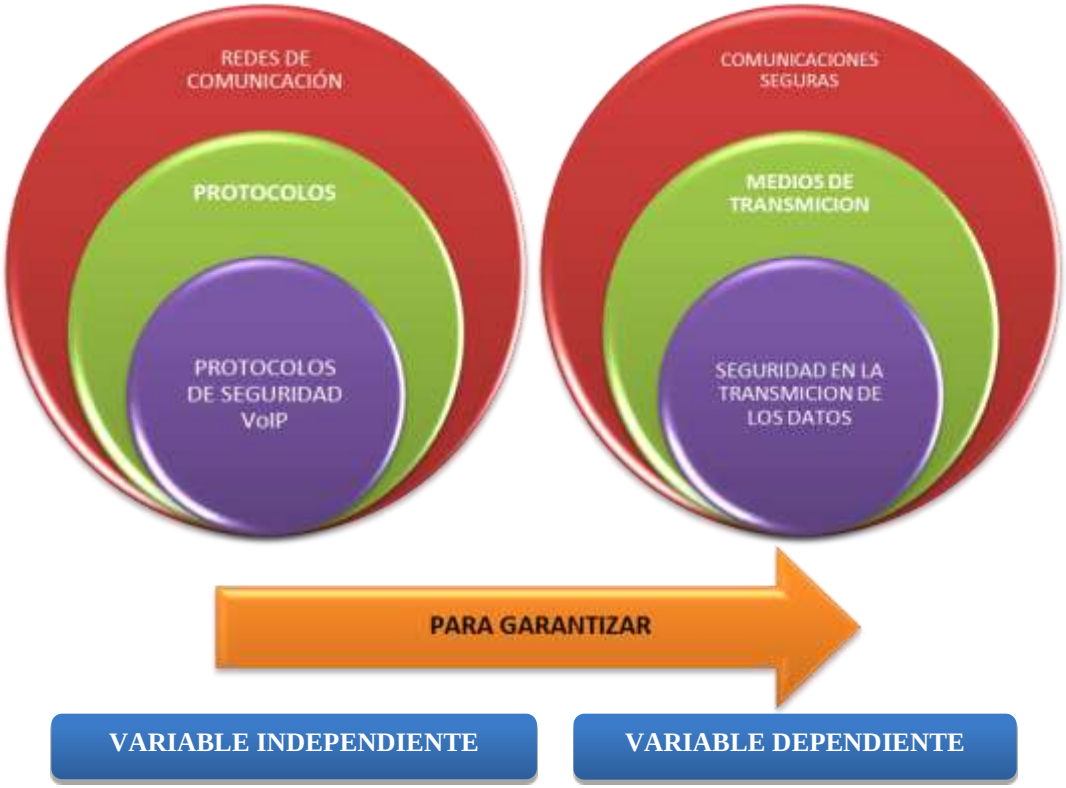


Figura No. 2.1: Organizador Lógico de Variables
Elaborado por: Freddy Robalino

Figura No. 2.2: Constelación de Ideas de la Variable Independiente
Elaborado por: E. Freddy Robalino

Figura No. 2.3: Constelación de Ideas de la Variable Dependiente
Elaborado por: E. Freddy Robalino P.

Categorías de la Variable Independiente

REDES DE COMUNICACIÓN

Definición

Las redes o infraestructuras de (tele) comunicaciones proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores.

Los elementos necesarios comprenden disponer de acceso a la red de comunicaciones, el transporte de la información y los medios y procedimientos (conmutación, señalización, y protocolos para poner en contacto a los extremos (abonados, usuarios, terminales,…) que desean intercambiar información. Además, numerosas veces los usuarios se encuentran en extremos pertenecientes a diferentes tipos de redes de comunicaciones, o en redes de comunicaciones que aun siendo iguales son de distinta propiedad. En estos casos, hace falta contar con un procedimiento de interconexión.

Arquitecturas de redes de comunicaciones distintas para distintos servicios

Entre la red telefónica, que hace posible que dos abonados mantengan una conversación de voz, y la red de difusión de televisión, mediante la que una estación de televisión emite sus programas desde sus estudios hasta los receptores de los televidentes, existen diferencias fundamentales en cuanto a la naturaleza del mensaje que se envía, el sentido de la transmisión, y el número y tipo de usuarios que intervienen. Telefonear es hablar con otra persona, es por tanto una comunicación interpersonal, mientras que ver la televisión es, por ejemplo, observar qué sucede en otro lugar remoto lo cual significa que hay un proveedor de contenido; estas diferencias condicionan la complejidad de las redes de comunicaciones involucradas, así como los elementos de los cuales se componen.

Siguiendo con el ejemplo utilizado, la diferencia fundamental entre ambos radica en que la red telefónica proporciona un camino para que se comuniquen cualesquiera dos abonados, mediante la marcación de un número que identifica unívocamente a cada terminal. Cualquier abonado puede comunicarse con cualquier otro y las redes telefónicas (fijas y móviles) extendidas por todo el mundo hacen esto posible. En la difusión de televisión, unas imágenes son transmitidas desde los estudios hasta los oportunos reemisores, que finalmente cubren una cierta zona mediante potentes antenas. Esta señal es recibida por los televidentes mediante otra antena y su receptor de televisión. La señal de televisión está siempre disponible y es voluntad del usuario acceder a la misma.

En un sistema de televisión convencional (tanto analógico como digital) el usuario no tiene ninguna posibilidad de interactuar con el extremo que envía la información.

Arquitecturas de las redes de comunicaciones.

Conmutación de circuitos y conmutación de paquetes

Las redes de comunicación se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Por ejemplo, existen necesidades de intercambio de información entre usuarios que obligan a mantener un flujo continuo de información, o al menos que la información llegue sin retardos apreciables para el usuario y sin desordenar, pues de lo contrario se altera su significado. Este es el caso de la voz o, en muchos casos, del vídeo.

También es posible utilizar arquitecturas que se basan en un flujo discontinuo de información formado por "paquetes" separados de datos. Estas arquitecturas son típicas de sistemas donde la información es discontinua de forma natural (como por ejemplo en el uso del correo electrónico), pero también se puede utilizar en aquellos sistemas que requieren un flujo continuo de información, siempre y cuando se garantice que la red de comunicaciones entrega la información sin un retardo apreciable para los usuarios y sin desordenar los paquetes de datos en los que se ha descompuesto el flujo de información.

Para que la información enviada por un terminal, sea recibida en el otro extremo, las redes (y las arquitecturas mediante las que se implementan) establecen un "camino" entre los extremos por el que viaja la información. Como las redes de comunicaciones no unen directamente a todos los usuarios con el resto, sino que tienen una estructura jerárquica, es necesario contar con un procedimiento de "conmutación" o "encaminamiento" que dirija la información (sea un flujo continuo o esté "paquetizada") hacia su destinatario.

Siguiendo con esta lógica, existen dos tipos básicos de arquitecturas de redes de comunicación: conmutación de circuitos y conmutación de paquetes. En la conmutación de circuitos, el camino (llamado "circuito") entre los extremos del proceso de comunicación se mantiene de forma permanente mientras dura la comunicación, de forma que es posible mantener un flujo continuo de información entre dichos extremos. Este es el caso de la telefonía convencional.

Su ventaja principal radica en que una vez establecido el circuito su disponibilidad es muy alta, puesto que se garantiza este camino entre ambos extremos independientemente del flujo de información. Su principal inconveniente reside en consumir muchos recursos del sistema mientras dura la comunicación, independientemente de lo que en la realidad pudiera requerir.

En la conmutación de paquetes, no existe un circuito permanente entre los extremos y, la red, simplemente, se dedica a encaminar paquete a paquete la información entre los usuarios. En la práctica esto significa que los paquetes en los que se ha dividido la información pueden seguir caminos diferentes. Su principal ventaja es que únicamente consume recursos del sistema cuando se envía (o se recibe) un paquete, quedando el sistema libre para manejar otros paquetes con otras información o de otros usuarios. Por tanto, la conmutación de paquetes permite inherentemente la compartición de recursos entre usuarios y entre informaciones de tipo y origen distinto.

Este es caso de Internet. Su inconveniente reside en las dificultades en el manejo de informaciones de "tiempo real", como la voz, es decir, que requieren que los paquetes de datos que la componen lleguen con un retardo apropiado y en el orden

requerido. Evidentemente las redes de conmutación de paquetes son capaces de manejar informaciones de "tiempo real", pero lo hacen a costa de incrementar su complejidad y sus capacidades.

Caracterización de las redes de comunicaciones.

Direccionalidad, ancho de banda y simetría, redes analógicas y digitales

En primer lugar las redes de comunicaciones se pueden distinguir en función de si el camino por el que circula la información es posible en ambos sentidos o uno solo. Así, se tienen:

a) Redes de comunicaciones unidireccionales en las que la información viaja desde un emisor a un receptor, no existiendo camino de retorno para la comunicación inversa. Este tipo de comunicaciones se suele encontrar en las redes de difusión o distribución.

b) Redes de comunicaciones bidireccionales o interactivas: la información entre los extremos viaja en los dos sentidos, típicamente por el mismo camino, aunque también existen redes en que no tiene por qué coincidir los caminos de ida y vuelta. Algunos ejemplos son las redes de telefonía y de datos.

c) Redes híbridas, en las que se integran tipos diferentes de redes; por ejemplo, una red unidireccional para un sentido de la comunicación es combinada con otra red para el camino de retorno. Estas soluciones fragmentarias permiten tener, por ejemplo, servicios interactivos de televisión, en la que ésta es recibida por la red de difusión terrestre o por satélite, mientras que las selecciones del usuario y sus peticiones de vídeo bajo demanda (VoD[11]), se envían por Internet (sobre la red telefónica).

En cuanto al ancho de banda, hay que señalar que los tipos de información que pueden circular por las redes son muy variados, en cuanto a su naturaleza, tratamiento, degradación y, particularmente de muy distinto ancho de banda.

Dentro del ancho de banda de una señal quedan recogidas todas las frecuencias distintas que incorpora la señal. Las variaciones de frecuencia de una señal de voz son muy inferiores a las de una imagen movimiento (vídeo). La tecnología requerida en cada caso es muy distinta; la frecuencia es la variable fundamental del diseño de sistemas de comunicaciones, en sus aspectos de transporte de señal. De aquí, se puede hablar de redes de banda ancha cuando la información que manejan ocupa un rango de frecuencias elevado y de banda estrecha en caso contrario.

Además, en determinados usos de las redes de comunicaciones, uno de los extremos genera mucha más información que el otro, lo que tiene implicaciones relativas a la ubicación de las infraestructuras de mayor ancho de banda, en el sentido emisor-receptor o en el inverso. El grado de simetría se refiere a la distribución del flujo de información entre los dos extremos de la comunicación, distinguiéndose entre redes asimétricas y redes simétricas. En las primeras uno de los extremos de la comunicación genera mucha mayor cantidad de información que la otra parte y el mayor ancho de banda mayor se situará en el camino de emisor a receptor, siendo muy inferior el dispuesto en sentido contrario.

Por último si la información y el manejo que se hace de la misma son en formato digital, se puede hablar de redes digitales. Por el contrario si la información y/o el manejo de la misma son analógicos, se trata de redes analógicas.

Tipos de redes de comunicaciones

Existen muchas formas posibles de clasificación de redes de comunicaciones. A continuación se consideran las más importantes. A este respecto hay que señalar que las clasificaciones siguientes no son excluyentes. Las redes de nueva generación (y, en general, las redes de conmutación de paquetes) tienen la capacidad de comportarse de formas diversas según el objetivo de uso que se persiga.

Redes de difusión y redes conmutadas

En función de que la información se reciba por un usuario determinado, un conjunto determinado de ellos, o un número indeterminado de los mismos, se tienen:

a) Redes de difusión: la información enviada se recibe en cualquier terminal conectado, recibiendo todos los usuarios la misma información y a la vez. El ejemplo típico son las redes de televisión convencionales en cualquiera de sus formas de transporte, cable, satélite o terrenal.

b) Redes conmutadas: cualquier usuario conectado a la red puede intercambiar información con cualquier otro conectado a la misma, mediante el establecimiento de la conexión entre los terminales extremos. El ejemplo más conocido son las redes de telefonía. El uso del correo electrónico sobre Internet es otro ejemplo de comportamiento punto a punto.

c) Entre estos dos casos hay varios intermedios. Por un lado están las redes de difusión con acceso condicional en las que la señal emitida por un transmisor es recibida por cualquier terminal conectado a la red, recibiendo los terminales la misma información y a la vez, pero a diferencia de las redes de difusión puras, cada usuario puede tener acceso a la información que personalmente ha solicitado al emisor mediante petición previa. La tecnología de acceso condicional es la que permite la personalización de los contenidos que el usuario recibe, incluso mediante las redes de difusión convencionales.

En este sentido, este tipo de redes actúan como redes de difusión virtualmente conmutadas. Por otro lado están las redes de multicasting en las que un conjunto determinado (y conocido) de usuarios recibe la misma información. De esta forma se ahorra capacidad de transmisión, ya que todos los usuarios involucrados comparten la misma información. La difusión audiovisual sobre Internet a veces utiliza algunos de estos mecanismos multicasting por el motivo señalado.

Redes punto a punto y redes multipunto

Esta clasificación considera los flujos de información con respecto a su origen y destino y es prácticamente paralela con la anterior. Se tienen:

a) redes punto a punto: un extremo (usuario) entabla comunicación con otro, y la arquitectura de la red mantiene separados y diferenciados estos flujos de información. Ejemplos típicos son la telefonía (fija o móvil).

b) punto a multipunto: un usuario o terminal mantiene un flujo de información simultáneamente con otros varios terminales. En caso de que los "usuarios multipunto" puedan generar información, la información que transmiten cada uno de ellos es recibida exclusivamente por el "usuario punto", quién a su discreción la hará visible al resto de "usuarios multipunto". Un ejemplo típico es la difusión de TV, o las aplicaciones de teleeducación por videoconferencia.

c) multipunto a multipunto: todos los usuarios pueden comunicarse simultáneamente con el resto. Un esquema de este tipo se encuentra en los sistemas de chat o también en los de juego en red.

Redes fijas, inalámbricas, móviles y celulares

Otro parámetro que caracteriza las redes de comunicaciones y condiciona su diseño es el grado de movilidad y el uso de espectro radioeléctrico de los extremos de la comunicación. Se tienen:

a) redes fijas: los usuarios y los terminales están permanentemente fijos, conectados físicamente a las redes mediante un cable o mediante espectro radioeléctrico, pero sin poder desplazarse de ubicación.

b) redes inalámbricas: utilizan espectro radioeléctrico para la comunicación

c) redes de móviles: los usuarios están en movimiento dentro de las zonas de cobertura de la red, y los terminales proporcionan a la red las señales que permiten

su seguimiento e identificación. Obsérvese que todas las redes de móviles son inalámbricas, pero no al revés.

d) redes celulares: son redes inalámbricas que tienen divida la zona de cobertura en "células" o "celdas[12]". Los sistemas de comunicaciones móviles (llamados de aquí sistemas de comunicaciones celulares) son un ejemplo típico.

Extensión de las redes

Redes locales, metropolitanas y de área extensa

También se pueden clasificar las redes en función del grado y extensión de la cobertura geográfica de la red, medida en términos de posibilidad de acceso a otros usuarios. Se tienen:

a) redes de cobertura local: la red tiene una cobertura reducida, siendo accesibles únicamente los usuarios dentro de la misma. Ejemplos son las LAN de datos, las centralitas telefónicas, las redes de radiotelefonía en grupo cerrado de usuarios (trunking) con cobertura local o los sistemas de buscapersonas.

b) redes de cobertura extensa: la red cubre un territorio amplio (regional, nacional e incluso internacional), siendo posible acceder a cualquier usuario de la misma. Ejemplos son las redes de telefonía fija, las de telefonía móvil, las redes de área extensa de datos (WAN), Internet o las redes globales por satélite.

c) redes metropolitanas: se trata de un caso intermedio entre ambas. El ejemplo típico son las redes MAN de datos.

PROTOCOLOS

Definición de Protocolo

Un protocolo es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos), es decir, es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red. Existen diversos protocolos de acuerdo a cómo se espera que

sea la comunicación. Algunos protocolos, por ejemplo, se especializarán en el intercambio de archivos (FTP[13]); otros pueden utilizarse simplemente para administrar el estado de la transmisión y los errores (como es el caso de ICMP[14]), etc.

En Internet, los protocolos utilizados pertenecen a una sucesión de protocolos o a un conjunto de protocolos relacionados entre sí. Este conjunto de protocolos se denomina TCP/IP. Entre otros, contiene los siguientes protocolos:
HTTP, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, Telnet, NNTP

Protocolo orientado a conexión y protocolo no orientado a conexión

Generalmente los protocolos se clasifican en dos categorías según el nivel de control de datos requerido:

Protocolos orientados a conexión

Estos protocolos controlan la transmisión de datos durante una comunicación establecida entre dos máquinas. En tal esquema, el equipo receptor envía acuses de recepción durante la comunicación, por lo cual el equipo remitente es responsable de la validez de los datos que está enviando. Los datos se envían entonces como flujo de datos. TCP es un protocolo orientado a conexión;

Protocolos no orientados a conexión: éste es un método de comunicación en el cual el equipo remitente envía datos sin avisarle al equipo receptor, y éste recibe los datos sin enviar una notificación de recepción al remitente. Los datos se envían entonces como bloques (datagramas). UDP[15] es un protocolo no orientado a conexión.

Protocolo y su implementación

Un protocolo define únicamente cómo deben comunicar los equipos, es decir, el formato y la secuencia de datos que van a intercambiar. Por el contrario, un protocolo no define cómo se programa el software para que sea compatible con el protocolo. Esto se denomina implementación o la conversión de un protocolo a un lenguaje de programación.

Las especificaciones de los protocolos nunca son exhaustivas. Asimismo, es común que las implementaciones estén sujetas a una determinada interpretación de las especificaciones, lo cual genera especificidades de ciertas implementaciones o, aún peor, incompatibilidad o fallas de seguridad.

PROTOCOLOS DE SEGURIDAD VoIP

Definición del Protocolo VoIP

Voz sobre Protocolo de Internet, también llamado Voz IP, VozIP, VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes, en lugar de enviarla en forma digital o analógica, a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local (LAN).

Objetivo del Protocolo VoIP

El objetivo del protocolo VoIP es dividir en paquetes los flujos de audio para transportarlos sobre redes basadas en IP .Los protocolos de las redes IP originalmente no fueron diseñados para el fluido el tiempo real de audio o cualquier otro tipo de medio de comunicación. La PSTN está diseñada para la transmisión de voz, sin embargo tiene sus limitaciones tecnológicas. Es por lo anterior que se crean los protocolos para VoIP, cuyo mecanismo de conexión abarca una serie de transacciones de señalización entre terminales que cargan dos flujos de audio para cada dirección de la conversación.

Protocolos VoIP utilizados

A algunos de los protocolos VoIP más importantes.

Figura No. 2.4: Algunos Protocolos VoIP
Rediseñado por: Freddy Robalino

SIP

Session Initiation Protocol.-Es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Fue desarrollado inicialmente en el grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control) y, a partir de Septiembre de 1999, pasó al grupo de trabajo IETF[16] SIP.

Este protocolo considera a cada conexión como un par y se encarga de negociar las capacidades entre ellos. Tiene una sintaxis simple, similar a HTTP o SMTP.
Posee un sistema de autenticación de pregunta/respuesta.

Tiene métodos para minimizar los ***efectos de DoS*** (Denial of Service o Denegación de Servicio), que consiste en saturar la red con solicitudes de invitación. Utiliza un mecanismo seguro de transporte mediante TLS. No tiene un adecuado direccionamiento de información para el funcionamiento con NAT.

H.323

Originalmente fue diseñado para el transporte de vídeo conferencia. Su especificación es compleja. Es un protocolo relativamente seguro, ya que utiliza RTP. Tiene dificultades con NAT, por ejemplo para recibir llamadas se necesita direccionar el puerto TCP 1720 al cliente, además de direccionar los puertos UDP para la media de RTP y los flujos de control de RTCP. Para más clientes detrás de un dispositivo NAT se necesita gatekeeper en modo proxy.

Interacción del protocolo H.323 con VoIP

Se decidió que el h.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del h.323, de tal forma que en caso de conflicto, y con el fin de evitar divergencias entre los estándares, se decidió que h.323 tendría prioridad sobre el VoIP. El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a la transmisión de señalización por tonos multifrecuencia (DTMF).

El protocolo H.323 es usado, por ejemplo, por NetMeeting para hacer llamadas IP. Este protocolo permite una gran variedad de elementos que interactúan entre ellos:

Terminales, son los clientes que inician una conexión VoIP. Estos usuarios solo pueden conectarse entre ellos, y si es necesario el acceso de un usuario adicional a la comunicación se necesitaran algunos elementos adicionales.

Gatekeepers, que operan básicamente de la siguiente manera: Servicio de traducción de direcciones (DNS), de tal manera que se puedan usar nombre en lugar de direcciones IP. **Autenticación y control de admisión**, para permitir o denegar el acceso de usuarios. **Administración del ancho de banda.** *Gateways*, puntos de referencia para conversión TCP/IP - PSTN.

Unidades de control multipunto (MCUS), para permitir la realización de conferencias.

Servicios

H.323 no permite solamente VoIP, sino también comunicación para intercambio de datos y video. El h.323 comprende también una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

Direccionamiento RAS:

RAS (registration, admission and status). Protocolo de comunicaciones que permite a una estación h.323 localizar otra estación h.323 a través del gatekeeper.
DNS (domainnameservice). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo ras pero a través de un servidor DNS.

Señalización q931:

q.931 señalización inicial de llamada.

h.225 control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz.

h.245 protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.

Compresión de voz g711:

Requeridos: g.711 y g.723

Opcionales: g.728, g.729 y g.722

Transmisión de voz UDP-TCP:

UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

RTP (real time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

Control de la transmisión RTCP:

RTCP (real time control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

Figura No. 2.5: Control de la transmisión RTCP
Rediseñado por: Freddy Robalino

Actualmente se puede partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, permitirán construir las aplicaciones VoIP.

Estos elementos son:

- Teléfonos IP.

- Adaptadores para PC.
- Hubs telefónicos.
- Gateways (pasarelas RTC / IP).
- Gatekeeper.
- Unidades de audio conferencia múltiple. (MCU voz)
- Servicios de directorio.

Diferencias entre SIP y H.323

- Entre las diferencias que podemos encontrar tenemos que el protocolo H.323 especifica servicios mientras que el protocolo SIP es un protocolo de señalización para dar base a servicios.
- H.323 engloba un amplio conjunto de protocolos de implementación obligatoria.
- La negociación de capacidades es más completa y compleja en H.323.
- H.323 define mecanismos de gestión y administración de la red.
- SIP está integrado en la infraestructura Web y proporciona servicios de mensajería instantánea.
- SIP tiene mejores mecanismos de detección de bucles, espirales y otros errores de configuración de la red.
- El 3gpp9 ha adoptado SIP como protocolo de señalización.
- Desde las primeras versiones, el inicio de llamadas es más rápido con SIP.

Tabla No. 1.1: Comparación entre H.323 y SIP

	H.323	SIP
Arquitectura	H.323 cubre casi todos los servicios como capacidad de intercambio, control de conferencia, señalización básica, calidad de servicio, registro, servicio de descubrimiento y más.	SIP es modular y cubre la señalización básica, la localización de usuarios y el registro. Otras características se implementan en protocolos separados.
Componentes	Terminal/Gateway	UA
	Gatekeeper	Servidores
Protocolos	RAS/Q.931	SI
	H.245	SDP
Funcionalidades de control de llamada		
Transferencia de llamada (Call Transfer)	Si	Si
Expedición de llamada (Call Forwarding)	Si	Si
Tenencia de llamada (Call Holding)	Si	Si
Llamada estacionada/recogida (Call Parking/Pickup)	Si	Si
Llamada en espera (Call Waiting)	Si	Si
Indicación de mensaje en espera (Message Waiting Indication)	Si	No
Identificación de nombre (Name Identification)	Si	No
Terminación de llamada con subscriptor ocupado (Call Completion on Busy Subscriber)	Si	Si
Ofrecimiento de llamada (Call Offer)	Si	No
Intrusión de llamada (Call Intrusión)	Si	No

	H.323 las divide en los protocolos H.450, RAS, H.245 y Q.931	
Características Avanzadas		
Señalización multicast (Multicast Signaling)	Si, requiere localización (LRQ) y descubrimiento automático del gatekeeper (GRQ).	Si, ejemplo, a través de mensajes de grupo INVITEs.
Control de la llamada de un tercero (Third-party Call Control)	Si, a través de pausa de la tercera parte y re-enrutando según está definido en H.323. Un control más sofisticado se define en el standard de las series H.450.x.	Si, según se describe en los borradores (Drafts) del protocolo.
Conferencia	Si	Si
Pinchar para llamar (Click for Dial)	Si	Si
Escalabilidad		
Número amplio de dominios (Large Number of Domains)	La intención inicial de H.323 fue el soporte de LANs, por lo que está pensado para el direccionamiento de redes amplias. El concepto de zona fue añadido para acomodar este direccionamiento amplio. Los procedimientos son definidos por localización de usuarios a través de nombres de email. El anexo G define la comunicación entre dominios administrativos, describiendo los métodos para resolución de direcciones, autorización de acceso y el reporte entre dominios administrativos. En las búsquedas multidominio no hay formas sencillas de detectar bucles. La detección de bucles se puede realizar a través del campo "PathValue" pero introduce problemas relativos a la escalabilidad.	SIP soporta de manera inherente direccionamientos de áreas. Cuando muchos servidores están implicados en una llamada SIP usa un algoritmo similar a BGP que puede ser usado en una manera sin estado evitando problemas de escalabilidad. Los SIP Registrar y servidores de redirección fueron diseñados para soportar localización de usuarios.

Gran cantidad de llamadas (Large Number of Calls)	El control de llamadas en se implementa de una manera sin estado. Un Gateway usa los mensajes definidos en H.225 para ayudar al gatekeeper en el balanceo de carga de los Gateways implicados.	El control de llamadas en se implementa de una manera sin estado. SIP soporta escalabilidad n a n entre UAs y servidores. SIP necesita menos ciclos de CPU para generar mensajes de señalización Por lo tanto, teóricamente un servidor puede manejar más transacciones. SIP ha especificado un método de balanceado de carga basado en el mecanismo de traslación DNS SRV.
Estado de la conexión	Con estado o sin estado.	Con estado o sin estado. Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte, pero sin embargo la señalización de llamadas tiene que ser terminada explícitamente.
Internacionalización	Si, H.323 usa Unicode (BMP String con ASN.1) para alguna información textual (h323-id), pero generalmente tiene pocos parámetros textuales	Si, SIP usa Unicode (ISO 10646-1), codificado como UTF-8, para todas las cadenas de texto, permitiendo todos los caracteres para nombres, mensajes y parámetros. SIP provee métodos para la indicación del idioma y preferencias del idioma.

Seguridad	Define mecanismos de seguridad y facilidades de negociación mediante H.235, puede usar SSL para seguridad en la capa de transporte.	SIP soporta autentificación de llamante y llamado mediante mecanismos HTTP. Autenticación criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP. Claves para encriptación multimedia se ofrecen usando SDP. SSL soporta autenticación simétrica y asimétrica. SIP también define autenticación y encriptación final usando PGP o S/MIME.
Interoperabilidad entre versiones	La compatibilidad hacia atrás de H.323 permite que todas las implementaciones basadas en diferentes versiones de H.323 sean fácilmente integrables.	En SIP, una nueva versión puede descartar características que no van a ser soportadas más. Esto consigue reducir el tamaño del código y la complejidad del protocolo, pero hace perder cierta compatibilidad entre versiones.
Implementación de la Interoperabilidad	H.323 provee una guía de implementación, que clarifica el standard y ayuda a la interoperabilidad entre diferentes implementaciones.	SIP no prevé ninguna guía de interoperabilidad

Facturación	Incluso con el modelo de llamada directa H.323, la posibilidad de facturar la llamada no se pierde porque los puntos finales reportan al gatekeeper el tiempo de inicio y finalización de la llamada mediante el protocolo RAS.	Si un proxy SIP quiere recoger información de facturación no tiene otra opción que revisar el canal de señalización de manera constante para detectar cuando se completa la llamada. Incluso así, las estadísticas están sesgadas porque la señalización de la llamada puede tener retardos.
Códecs	H.323 suporta cualquier codec, estandarizado o propietario, no sólo códecs ITU-T, por ejemplo códecs MPEG o GSM. Muchos fabricantes soportan códecs propietarios a través de ASN.1 que es equivalente en SIP a "códigos privados de mutuo acuerdo" Cualquier codec puede ser señalizado a través de la característica Generic Capability añadida en H.323v3.	SIP soporta cualquier codec IANA-registered (es una característica heredada) o cualquier codec cuyo nombre sea de mutuo acuerdo.
Bifurcación de llamadas (Call Forking)	Un gatekeeper H.323 puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.	Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.
Protocolo de transporte	Fiable (Reliable) o no fiable (unreliable), ej., TCP o UDP. La mayoría de las entidades H.323 usan transporte fiable (TCP) para señalización.	Fiable (Reliable) o no fiable (unreliable), ej., TCP o UDP. La mayoría de las entidades SIP usan transporte no fiable (UDP) para señalización.
Codificación de mensajes (Message Encoding)	H.323 codifica los mensajes en un formato binario compacto adecuado para conexiones de gran ancho de banda.	SIP codifica los mensajes en formato ASCII, adecuado para que lo puedan leer los humanos.
Direccionamiento (Addressing)	Mecanismos de señalización flexibles, incluyendo URLs y números E.164.	SIP sólo entiende direcciones del estilo URL.

Interconexión Red Telefónica Pública (PSTN Internetworking)	H.323 toma prestado de la red telefónica pública protocolos como Q.931 y está por tanto bien adecuada para la integración. Sin embargo, H.323 no emplea la analogía a tecnología de conmutación de circuitos de red telefónica pública de SIP. H.323 es totalmente una red de conmutación de paquetes. El cómo los controles deben implementarse en la arquitectura H.323 está bien recogido en el estándar.	SIP no tiene nada en común con la red telefónica pública y esa señalización debe ser "simulada" en SIP. SIP no tiene ninguna arquitectura que describa cómo deben implementarse los controles.
Detección de bucles (Loop Detection)	Si, los gatekeepers pueden detectar bucles mirando los campos "Call Identifier" y "destination Address" en los mensajes de procesamiento de la llamada. Combinando ambos se pueden detectar bucles	Si, el campo "Vía" de la cabecera de los mensajes SIP facilita el proceso. Sin embargo, este campo "Vía" puede generar complejidad en los algoritmos de detección de bucles y se prefiere usar la cabecera "Max-Forwards" para limitar el número de saltos y por tanto los bucles.
Puertos mínimos para una llamada VoIP	5 (Señalización de llamada, 2 RTP, and 2 RTCP.)	5 (Señalización de llamada, 2 RTP, and 2 RTCP.)
Conferencias de vídeo y datos	H.323 suporta todo tipo de conferencia de vídeo y datos. Los procedimientos permiten control de la conferencia y sincronización de los streams de audio y vídeo,	SIP no soporta protocolos de vídeo como T.120 y no tiene ningún protocolo para control de la conferencia.

Elaborado por: Freddy Robalino

H323 es el protocolo más definido pero adolece de cierta falta de flexibilidad. SIP está menos definido pero es más fácil de integrar, ¿Que protocolo ganará al final? Es difícil de decir en este momento pero dependerá de la aplicación que se quiera desarrollar. (SIP es más fácil de implementar aunque los conceptos de H.323 son mejores).

Fallas encontradas

A pesar de las advertencias de que VoIP es vulnerable a un conjunto de ataques inherentes a sus características, las mayores amenazas recaen en debilidades de seguridad propias de las redes TCP/IP: gusanos, virus y el uso de vulnerabilidades sobre la tecnología, pueden congestionar o colapsar las redes que sustentan VoIP. Por ejemplo, algunas IP PBX están basadas en Windows o Unix, por lo cual toda brecha de seguridad en estos sistemas operativos afecta directamente al servicio.

Las fallas que comúnmente afectan a VoIP son:

- Continuidad del servicio
- Confidencialidad de la información
- Forjamiento de la identidad del usuario

Tipos de Seguridad

Uno de los problemas más comunes cuando nos referimos a la seguridad de VoIP es tratar esta tecnología como si fuera un tipo de aplicación común dentro de las redes IP. VoIP tiene otras demandas de seguridad, para VoIP es de alta prioridad el tiempo real y la calidad del servicio que se brinda.
La siguiente lista son reglas que permiten establecer un tipo de seguridad VoIP.

1. Actualizar los parches de seguridad.

Hay que actualizar los programas expuestos a la red para evitar riesgos innecesarios. Algunos de los ataques de red pueden ser evitados actualizando los parches de seguridad.

2. Instalar un buen Antivirus.

Una de los mejores tipos de seguridad es un buen antivirus y tenerlo actualizado constantemente. Debido al crecimiento de virus y gusanos. Una de las razones por las cuales es combinar un buen antivirus con VoIP es que es que los sistemas de antivirus protegen los componentes VoIP de infecciones de computadoras que están vulnerables en la red.

3. Sistemas de detección y prevención de intrusos.

Usar un sistema de detección y prevención de intrusos es una técnica que permite proteger contra los ataques presentes en la capa de aplicación y red del modelo OSI. Estos sistemas incorporan técnicas como protocolos de detección de anomalías, reconocimientos de ataques, detección de puertas traseras y otros.

4. Instalar Gateways de capa de aplicación (ALGs) entre zonas seguras y no-seguras.

Estos Gateways son diseñados específicamente para manejar demanda de aplicaciones como aplicaciones VoIP. Pueden prevenir contra ataque maliciosos de otros sistemas.

5. Autentificación, Autorización e IPSec.

Se utiliza autentificaron y autorización para los protocolos VoIP basados en textos (SIP). Que son muy vulnerables a ataques en la red. IPSec provee de una capa adicional de seguridad en la capa de red, permitiendo encriptar y autentificar todos los paquetes.

6. Utilizar VPNs (Virtual Private Networks)

Al usar VPNs reducimos el riesgo de que las conversaciones puedan ser escuchadas (aunque el proceso de encriptación y desencriptación aumenta el consumo de ancho de banda e incrementa la latencia)
Por esto es aconsejable hacer VPN segmentado, es decir seleccionar las zonas por las que viajan los paquetes en las cuales no es segura su transmisión y ahí aplicar VPN con sus protocolos de seguridad.

7. Usar VLANs (Virtual LANs)

Ayuda a priorizar el tráfico de voz, segmentando el tráfico de datos y voz. Resultando en una baja latencia y mejor calidad.

8. Proteger contra inundaciones UDP

Este es un ataque en la red que ocurre cuando un paquete UDP es enviado con la intención de hacer caer los sistemas. Una solución es instalar Firewalls que tengan la opción de proteger contra estos ataques.

Categorías de la Variable Dependiente

COMUNICACIONES SEGURAS

Definición de Comunicación Segura

Es el proceso de transmisión y recepción de ideas, información y mensajes de manera segura. En los últimos 150 años, y en especial en las dos últimas décadas, la reducción de los tiempos de transmisión de la información a distancia y de acceso a la información de carácter confiable, ha supuesto uno de los retos esenciales de nuestra sociedad.

Comunicación segura en la red datos

La comunicación por medio de una red se lleva a cabo en dos diferentes categorías: la capa física y la capa lógica. La capa física incluye todos los elementos de los que hace uso un equipo para comunicarse con otros equipos dentro de la red, como, por ejemplo, las tarjetas de red, los cables, las antenas, etc.

La comunicación segura en redes datos se a través de la capa física y esta se rige por normas muy rudimentarias que por sí mismas resultan de escasa utilidad. Sin embargo, haciendo uso de dichas normas es posible construir los denominados *protocolos seguros*, que son normas de comunicación más complejas (mejor conocidas como de alto nivel), capaces de proporcionar servicios que resultan útiles.

La razón más importante (quizá la única) sobre por qué existe diferenciación entre la capa física y la lógica es sencilla: cuando existe una división entre ambas, es posible utilizar un número casi infinito de protocolos de distinto tipo y nivel de seguridad, lo que facilita la seguridad, actualización y migración entre distintas tecnologías y medios de transmisión.

MEDIOS DE TRANSMISIÓN

Definición de Medios de transmisión

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos. Distinguimos dos tipos de medios: guiados y no guiados. En ambos casos la transmisión se realiza por medio de ondas electromagnéticas. Los medios guiados conducen (guían) las ondas a través de un camino físico, ejemplos de estos medios son el cable coaxial, la fibra óptica y el par trenzado. Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen; como ejemplo de ellos tenemos el aire y el vacío.

La naturaleza del medio junto con la de la señal que se transmite a través de él constituye los factores determinantes de las características y la calidad de la transmisión. En el caso de medios guiados es el propio medio el que determina el que determina principalmente las limitaciones de la transmisión: velocidad de transmisión de los datos, ancho de banda que puede soportar y espaciado entre repetidores. Sin embargo, al utilizar medios no guiados resulta más determinante en la transmisión el espectro de frecuencia de la señal producida por la antena que el propio medio de transmisión.

Algunos medios de transmisión guiados son:

Pares trenzados

Este consiste en dos alambres de cobre aislados, en general de 1mm de espesor. Los alambres se entrelazan en forma helicoidal, como en una molécula de DNA. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios megabits, en distancias de pocos kilómetros. Debido a su adecuado comportamiento y bajo costo, los pares trenzados se utilizan ampliamente y es probable que se presencia permanezca por muchos años.

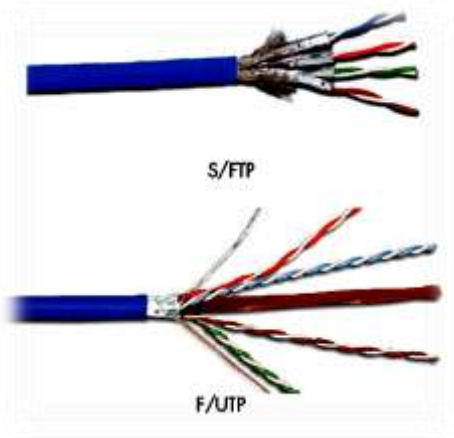


Figura No. 2.6: Pares trenzados

Diseñado por: The Siemon Company

Cable coaxial

El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante. Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector.

La construcción del cable coaxial produce una buena combinación y un gran ancho de banda y una excelente inmunidad al ruido. El ancho de banda que se puede obtener depende de la longitud del cable; para cables de 1km, por ejemplo, es factible obtener velocidades de datos de hasta 10Mbps, y en cables de longitudes menores, es posible obtener velocidades superiores. Se pueden utilizar cables con mayor longitud, pero se obtienen velocidades muy bajas. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de largas distancia del sistema telefónico.

Figura No. 2.7: Tipos de Cables Coaxiales
Diseñado por: Creative Commons

Fibra óptica

Un cable de fibra óptica consta de tres secciones concéntricas. La más interna, el núcleo, consiste en una o más hebras o fibras hechas de cristal o plástico. Cada

una de ellas lleva un revestimiento de cristal o plástico con propiedades ópticas distintas a las del núcleo. La capa más exterior, que recubre una o más fibras, debe ser de un material opaco y resistente.

Un sistema de transmisión por fibra óptica está formado por una fuente luminosa muy monocromática (generalmente un láser), la fibra encargada de transmitir la señal luminosa y un fotodiodo que reconstruye la señal eléctrica.

Figura No. 2.8: Tipos de Cables Coaxiales
Diseñado por: Creative Commons

Algunos medios no guiados:

Radio enlaces de VHF y UHF

Estas bandas cubren aproximadamente desde 55 a 550 MHz Son también omnidireccionales, pero a diferencia de las anteriores la ionosfera es transparente a ellas. Su alcance máximo es de un centenar de kilómetros, y las velocidades que permite del orden de los 9600 bps. Su aplicación suele estar relacionada con los radioaficionados y con equipos de comunicación militares, también la televisión y los aviones.

Microondas

Además de su aplicación en hornos, las microondas nos permiten transmisiones tanto terrestres como con satélites. Dada sus frecuencias, del orden de 1 a 10 GHz, las microondas son muy direccionales y sólo se pueden emplear en situaciones en que existe una línea visual que une emisor y receptor. Los enlaces de microondas permiten grandes velocidades de transmisión, del orden de 10 Mbps

Figura No. 2.9: Antena Satelital – Radio Enlace
Diseñado por: rigosky

SEGURIDAD EN LA TRANSMISIÓN DE LOS DATOS

Definición seguridad

La seguridad de este tipo datos (voz) se basa en el hecho de poder encriptar los mensajes (datos) que se envían por la red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos. Para llevar a cabo esta seguridad se crearon diversos protocolos se seguridad VoIP basados en esta idea.

En una red insegura, se pueden incrementar los controles en la seguridad para suplir las deficiencias. La realidad muestra que resulta más beneficioso considerar la mejora en la seguridad de la transmisión de los datos en la red, ya que de esta

forma se evitarán sistemas y aplicaciones robustas, redundando además en una sustancial mejora en la performance y los costos.
Para tener la visión clara de lo que se está investigando hay que entender algunos conceptos

Tendencias y objetivos de las vulnerabilidades de VoIP

Según la empresa McAfee Labs primera vez que se observó un incremento en las vulnerabilidades de VoIP fue a finales de 2006 y, desde entonces, la tendencia alcista se ha mantenido hasta la actualidad. En parte, podemos atribuir este aumento a la disponibilidad de mejores herramientas para detectar vulnerabilidades en VoIP, aunque, en gran medida, debe achacarse al creciente número de instalaciones VoIP (mayor disponibilidad). Según un informe de Infonetics Research, el conjunto de la telefonía para empresas creció más del 8% durante el segundo y el tercer trimestre de 2008. Cisco, Avaya y Nortel encabezan sistemáticamente la lista de los principales distribuidores para empresas.

En los últimos tiempos Cisco ha ocupado el primer puesto con un crecimiento del 19% durante el tercer trimestre de 2008. Avaya ha crecido un 10% y Nortel les sigue en tercera posición3. No es de extrañar que los productos de estos tres distribuidores reúnan la mayoría de las vulnerabilidades de VoIP conocidas.

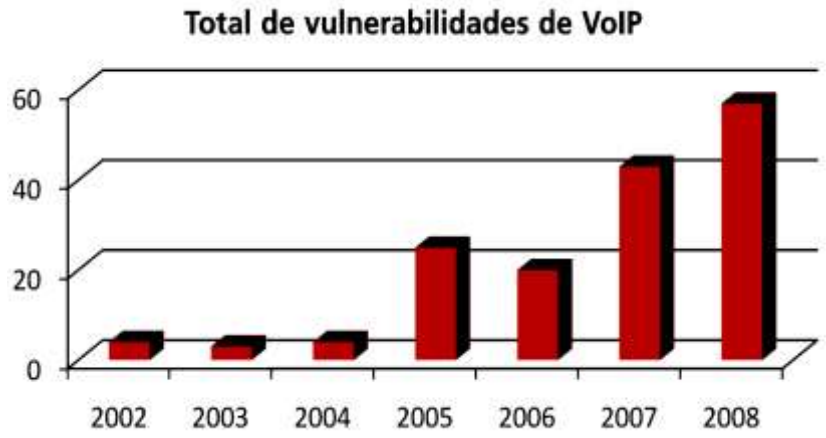


Figura No. 2.10: Total de vulnerabilidades en alza

Rediseñado por: Freddy Robalino

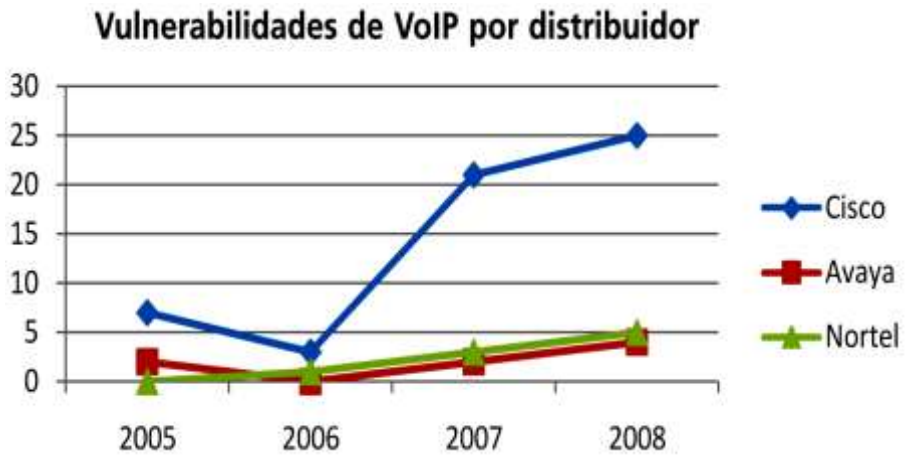


Figura No. 2.11: Cisco Lidera el campo
Diseñado por: Fuente: NVD

¿Cómo se producen los ataques?

Realización de llamadas VoIP

Para entender cómo se producen los ataques, hay que entender cómo funciona la arquitectura VoIP. La siguiente figura muestra los componentes de una llamada, desde el momento en que un usuario inicia una comunicación telefónica con otro usuario (1). La solicitud se envía al software de gestión de llamadas mediante una petición INVITE del protocolo de señalización/SIP (2). Recibida la petición, el software de gestión de llamadas localiza el destinatario y le reenvía la solicitud.

En ese momento, el control pasa a los dos usuarios, y el protocolo de transmisión multimedia/protocolo RTP codifica y transmite la conversación multimedia. En este ejemplo se emplea el protocolo SIP, aunque en otros entornos VoIP las etapas son similares.

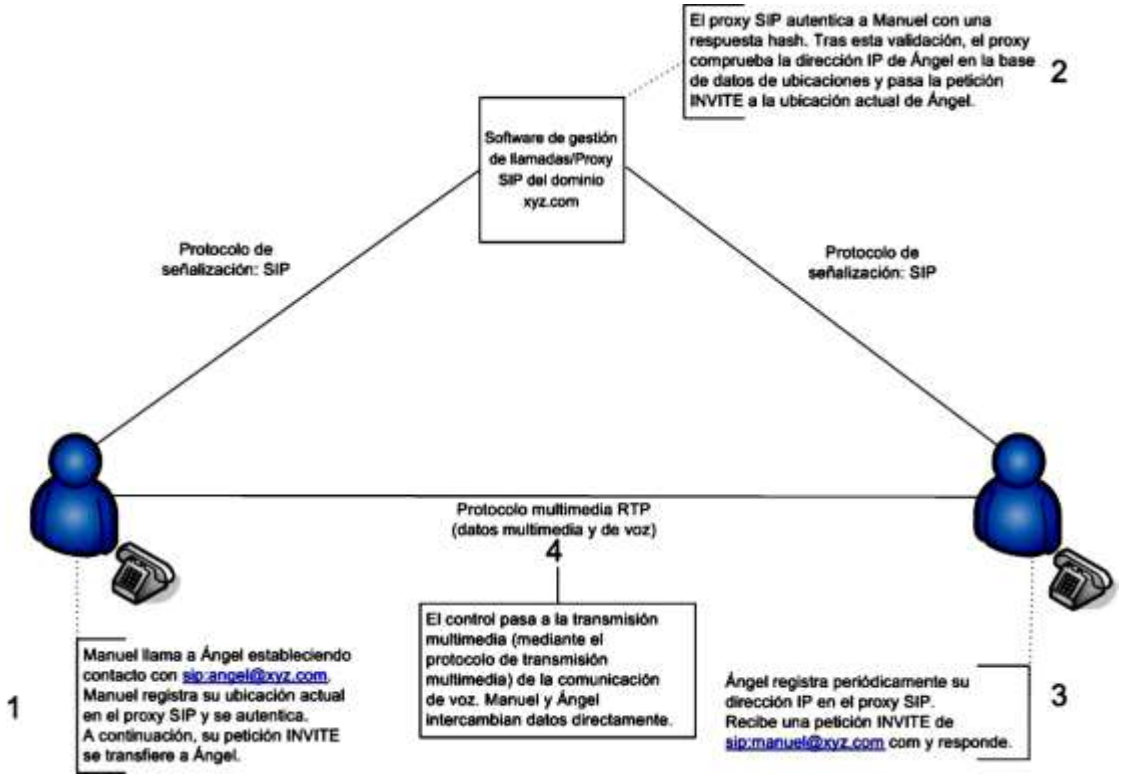


Figura No. 2.12: VoIP en acción, con el protocolo SIP
Rediseñado por: Freddy Robalino

Varias etapas de este proceso están expuestas a vulnerabilidades tales como la denegación de servicio de las peticiones INVITE, la interceptación de la conversación entre dos usuarios y las brechas en el software de gestión de llamadas. Vamos a analizar estos ataques y vulnerabilidades.

Ataques a nivel de protocolos

Escuchas ilegales o interceptación

En el 2001 se publicó una advertencia de la presencia de VOMIT (Voice Over Mis configured Internet Telephones, voz sobre teléfonos mal configurados en Internet). Esta herramienta extrae del tráfico de la red un volcado de una conversación con un teléfono IP de Cisco y lo convierte en un archivo que puede oírse en un reproductor de sonido normal. VOMIT sólo podía utilizarse con el

protocolo H.323/G.711 o con teléfonos IP de Cisco, aunque otras herramientas como VoIPong funcionan con SIP y el protocolo de transmisión multimedia/RTP.

Repetición

Los ataques de repetición reproducen ante la víctima una sesión legítima (captada normalmente interceptando el tráfico de la red). Con VoIP, los ataques de repetición se producen en el protocolo de señalización SIP. Hay un ataque bien conocido que utiliza técnicas de repetición para secuestrar la información de registro. El protocolo SIP emplea el comando de registro para indicar al software de gestión de llamadas dónde se encuentra un usuario en función de su dirección IP. El atacante puede reproducir esta solicitud y sustituir otra dirección IP para desviar todas las llamadas a su propia dirección.

Los ataques de repetición se producen porque hay partes del protocolo SIP que se comunican en texto normal.

Denegación de servicio

Dado que VoIP es un servicio de la red IP, está expuesto a los mismos ataques por inundación (*flooding*) que afectan a otros servicios basados en IP. Los ataques a infraestructuras incluyen la inundación de dispositivos telefónicos PBX IP VoIP y VoIP con andanadas de paquetes TCP SYN/UDP (User Datagram Protocol). En la comunidad de los hackers también son famosos los ataques a protocolos de señalización y multimedia con herramientas que, por ejemplo, envían oleadas de peticiones INVITE de SIP a un teléfono IP para agotar sus recursos (*flooder*) o inyectan peticiones BYE en un flujo de red para poner fin a una llamada ("Teardown").

Los agresores utilizan este tipo de ataques de *denegación de servicio* como forma de extorsión. Se considera que el servicio telefónico tradicional tiene una disponibilidad del 99,999% (los "cinco nueves" de la telefonía) y cabe esperar que

VoIP alcance la misma cifra. Sin embargo, VoIP está expuesto a ataques por inundación (mediante redes de bots y otras herramientas) y en los equipos de VoIP residen numerosas vulnerabilidades de denegación de servicio.

Manipulación de señales y transmisiones multimedia

Una vez más, dado que VoIP es un servicio de la red IP, es vulnerable a los mismos ataques de manipulación de redes que otros servicios de red. Uno de ellos es "RTP InsertSound", que permite a un intruso insertar archivos de sonido en una transmisión multimedia con RTP (conversación de voz entre dos o más teléfonos IP).

Ataques a nivel de aplicaciones

Dispositivos VoIP con servicios abiertos

Muchos teléfonos tienen un puerto de servicio abierto para que los administradores puedan recopilar estadísticas, información y ajustes de configuración remota. Estos puertos abren la puerta a la divulgación de información que los agresores pueden utilizar para conocer mejor la red e identificar los teléfonos VoIP.

Servicios Web de teléfonos VoIP

Un número importante de los puertos de servicio en los teléfonos VoIP que ponen los datos en riesgo también interaccionan como servicios Web y, por lo tanto, son susceptibles de sufrir las vulnerabilidades habituales, como la falsificación de peticiones y las secuencias de comandos entre sitios. La primera se produce cuando se inserta un vínculo en una página Web que utiliza las credenciales de la víctima, normalmente en una cookie.

A título de ejemplo, podemos citar la vulnerabilidad que se encontró hace poco en los teléfonos SIP de Snom Technology. Dicha vulnerabilidad permite a los usuarios cambiar la configuración del dispositivo, ver el historial de llamadas e incluso hacer llamadas telefónicas mediante una interfaz Web incorporada. Basta con que el agresor conozca la dirección IP del dispositivo VoIP para que se produzca un ataque. No tiene más que atraer al usuario del teléfono a un sitio malicioso y hacerse con sus credenciales para acceder después al teléfono con su dirección IP, como si fuera el propietario. Este método es particularmente insidioso porque neutraliza el firewall.

Vishing (VoIP phishing)

La verificación de la información personal por teléfono no es algo nuevo y, en general, estamos acostumbrados a no desconfiar de la identidad del que realiza la llamada. En el caso de las llamadas tradicionales, a menudo podemos rastrear su origen geográfico y solemos fiarnos del ID de la persona que efectúa la llamada para su identificación. Con VoIP esta seguridad desaparece. Las llamadas pueden venir de cualquier lugar de Internet y la verificación del ID del llamante puede falsificarse.

Los ciber delincuentes actuales aprovechan este anonimato con técnicas de "Vishing", es decir, la combinación entre VoIP y la falsificación de ID de la persona que efectúa la llamada. Al igual que ocurre con el phishing, el ataque de Vishing suele adoptar la apariencia de una institución financiera que pide información personal, como el número de la tarjeta de crédito o del documento de identidad. Nos han llegado informes sobre varios de estos ataques. En un ejemplo reciente, un mensaje de correo electrónico que parecía proceder de un banco ofrecía un número VoIP local como contacto.

El hecho de que el número fuese local daba legitimidad al mensaje. Si los ID de los llamantes son tan fáciles de falsificar y resulta tan sencillo crear números VoIP, prevemos que habrá muchos más ataques de ingeniería social de este tipo.

Spam VoIP

Al igual que el servicio telefónico estándar, VoIP también es objeto de comunicaciones no solicitadas ni deseadas.

El Spam VoIP también se conoce como SPIT (Spam over Internet Telephony, Spam en telefonía por Internet). Los agentes de tele marketing se han percatado del potencial de VoIP y de la conveniencia de utilizar la automatización para llegar a miles de usuarios. Estas llamadas no deseadas pueden consumir recursos rápidamente y generar un ataque de denegación de servicio. Para reducir los riesgos del SPIT basta con aplicar las lecciones aprendidas con el correo electrónico y el servicio telefónico tradicional (autenticación, listas blancas, etc.).

Fraude telefónico mediante VoIP

El fraude mediante VoIP consiste en obtener acceso a una red VoIP (gestor de llamadas o Gateway) y realizar llamadas no autorizadas (normalmente de larga distancia o internacionales). Los atacantes aprovechan el uso de nombres de usuario y contraseñas fáciles, Gateways abiertos y otros ataques a nivel de aplicaciones descritos en este informe. Este tipo de fraude es uno de los ataques más frecuentes contra la tecnología VoIP.

Los agresores atacan pequeñas empresas, como en Perth, Australia, donde realizaron 11.000 llamadas con un coste de más de 120.000 dólares americanos11, o roban más de 120 millones de minutos VoIP a compañías como Verizon y AT&T con un beneficio de 1,2 millones de dólares.

Requerimientos de Seguridad

Ya que son bien conocidas las vulnerabilidades de las redes IP sobre las que se envía los paquetes de voz, hay algunas recomendaciones o requerimientos de seguridad a la hora de implementar VoIP:

1. Protección de la privacidad de la conversación de la llamada
2. Autentificación de las entidades finales de la llamada
3. Protección contra el uso erróneo de los recursos de la red
4. Asegurar la facturación correcta por el proveedor de servicio, y protección de la información de la facturación contra el acceso no autorizado.
5. Protección del comportamiento del llamador o de la información estadística contra el acceso no autorizado.
6. Protección de los servidores de la red y los terminales contra amenazas bien conocidas tales como "negación del servicio" y "ataque del hombre en el medio".
Aunque no puede haber un sistema completamente seguro, sí hay que tomar ciertas medidas para que las vulnerabilidades sean mínimas.

IPSec

Protocolo IPSec (Internet Protocol Security), desarrollado por la IETF provee seguridad a redes que transmiten información que viaja desprotegida, como las redes de Internet. IPSec actúa en la capa de red, protegiendo y autentificando paquetes IP.

En general IPSec provee de los siguientes servicios de seguridad.

- Confiabilidad de datos.- Los paquetes enviados son cifrados antes de ser enviados a través de la red.
- Integridad de datos.- El que recibe los paquetes puede autentificar al que envía y asegurarse que el paquete no haya sido modificado.
- Autentificación de los datos de origen.- El que recibe los datos puede autentificar el origen de los paquetes IPSec enviados.
- Anti-replay.- El que recibe los paquetes IPSec puede detectar y rechazar paquetes retransmitidos.

Con IPSec los datos transmitidos cruzan las redes públicas sin temor de ser observados o atrapados.

Hipótesis

Los protocolos de VoIP inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A.

Señalamiento de Variables

Variable Independiente: Protocolos de VoIP

Variable Dependiente: Seguridad en la transmisión de datos.

CAPITULO III

Metodología

Enfoque

La presente investigación está enmarcada dentro del paradigma crítico propositivo, por lo tanto tendrá un enfoque cuali-cuantitativa

Investigación cualitativa por ser participativa, humanística, interna, interpretativa, con perspectiva desde adentro y asume una realidad dinámica.

Y cuantitativa por ser normativa, externa, explicativa, realista, orientado a la comprobación de la hipótesis que asume una realidad estable.

Modalidad de Investigación

Para el desarrollo de la investigación se utilizará las siguientes modalidades: La bibliográfica que aportará la información y permitirá la recolección de datos científicos de libros, documentos y artículos publicados en Internet y la Segunda modalidad la de campo: La cual permitirá determinar cuáles son los protocolos de VoIP implementados en la F.I.S.E.I.

Niveles o Tipos

El tipo de investigación al cual se llegará es el descriptivo, puesto que se nombrará los principales protocolos de VoIP así como las características y estándares adyacentes a la tecnología, además de las seguridades que proporcionan y las ventajas de utilizarlos e implementarlos en la transmisión de datos.

Población y Muestra

La población con la cual se trabajara corresponde a los administradores de la red laboratoristas y directores del CTT y UOCENIC. Por tal razón no existe muestra debido a que el universo es muy reducido.

Tabla No. 3.1: Población

Personal	Frecuencia
Administradores de la Red	**1**
Ayudantes de Laboratorio	**8**
Directores	**2**
Total	**11**

Elaborado por: Freddy Robalino

Operacionalización de Variables

Variable Independiente:

Tabla No. 3.2: Protocolos de VoIP

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (Emisor y receptor). A estos protocolos los gobiernan estándares, modos de acceso, secuencias temporales, etc.	NORMAS	Datos Audio Video	¿Existen normas que Regulen transmisión de información?	Encuesta / Cuestionario
	TRANSMISIÓN DE DATOS	Seguridad Eficiencia	¿Se logra de manera eficiente la transmisión de los datos ?	Encuesta / Cuestionario
	COMUNICACIÓN	Optima Buena Mala	¿La comunicación entre el emisor y el receptor es optima en todo momento?	Encuesta / Cuestionario
	MODOS DE ACCESO	Seguro Fácil acceso	¿El modo de acceso que utilizan los protocolos es el mas recomendado?	Encuesta / Cuestionario

Variable Dependiente:

Tabla No. 3.3: Seguridad en la Transmisión de Datos

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Es el tipo de seguridad y mecanismos de transporte que se le dan a los datos que trasmitimos por la red, para que llegue a su destino sin haber sido capturados, o modificados por nadie más que el destinatario, de manera que el usuario se sienta seguro.	TIPOS DE SEGURIDAD	Hardware Software H / S	¿Qué tipos de seguridades se dan a los datos?	Encuesta / Cuestionario
	MECANISMOS DE TRANSPORTE	Protocolos Encriptación IDS	¿Cuáles son los mecanismo de transporte tienen los datos?	Encuesta / Cuestionario
	TRANSMISIÓN DE DATOS	Seguridad Eficiencia	¿Se logra de manera eficiente la transmisión de los datos?	Encuesta / Cuestionario
	NIVEL DE SEGURIDAD	Alto Medio Bajo	¿Los usuarios se sienten confiados con el nivel de seguridad proporcionado para sus comunicaciones?	Encuesta / Cuestionario

Técnicas e Instrumentos

Encuesta con Cuestionario
Entrevista con Guía de la entrevista

Plan para Recolección de la Información

Los instrumentos que se utilizaron para la recolección y registro de la información fueron por medio de entrevistas, encuestas, etc.

El uso de Internet buscando al mejores alternativas que existe en carretera de la información virtual, es en la actualidad fundamental para la investigación realizada, complementada siempre por los documentos como Tesis, libros, revistas, catálogos de productos, etc.

Plan para el Procesamiento de la Información

Los datos recogidos se transformaron siguiendo los siguientes procedimientos:

- Revisión de la información.
- Realización de tabulación y tablas
- Manejo de la información.
- Estudio estadístico de los datos para la presentación de los resultados.

Una vez aplicados los instrumentos y analizada la validez, se procedió a la tabulación de datos. Acto seguido se procedió al análisis integral, enriquecido gracias a los elementos de juicio desprendidos del marco teórico, objetivos y variables de la investigación.

A continuación se efectuó la estructuración de conclusiones y recomendaciones que organizadas en una propuesta lógica y factible, permitirán participar proactivamente en la solución o minimización de la problemática planteada.

Finalmente, como parte medular de la investigación crítica propositiva, se estructura una propuesta pertinente al tema de investigación que nos compete, enfocada a optimizar de los recursos existentes, fiabilidad, confiabilidad y desempeño de la red de datos de la facultad sin perder de vista los objetivos trazados.

ENCUESTA A DIRECTORES Y USUARIOS DEL SERVICIO Y LA RED

Lugar de aplicación de Encuesta: _____

Objetivo de la Encuesta.- Determinar la incidencia de los protocolos en la seguridad de la red al transmitir los datos

Sus respuestas le permitirán al investigador

-Desarrollar un trabajo real y efectivo.

- Agradecemos su colaboración

Tabla No. 3.4: Encuesta Directores y Usuarios del Servicio y la Red

PREGUNTA	SI	NO
¿Ha tenido en cuenta la posibilidad de perder información, que se la roben, que no sea correcta?		
¿Sabe Ud. si existen controles que detecten posibles fallos en la seguridad?		
¿Conoce Ud. si existe un procedimiento de cifrado (seguridad) de las comunicaciones?		
¿Existen reglas que regulen la transmisión de voz en sus enlaces?		
¿Conoce si existen reglas que brinden seguridad en la transmisión de archivos (Datos) en sus enlaces?		
¿Sabe si se utiliza algún medio para priorizar el tráfico de las aplicaciones de voz?		
¿La transmisión y seguridad en sus enlaces para la transmisión de datos es eficiente?		
¿La transmisión y seguridad de sus datos es segura?		
¿La transferencia y seguridad de datos en los enlaces de comunicación es eficiente y confiable?		

¿Ha tenido problemas en la transmisión de aplicaciones de voz cuando se satura el canal de comunicación?		
¿Tienen un mecanismo de transporte los datos?		

ENCUESTA A ADMINISTRADORES DE REDES Y LABORATORISTAS

Lugar de aplicación de Encuesta: _____

Objetivo de la Encuesta.- Determinar la incidencia de los protocolos en la seguridad de la red al transmitir los datos

Sus respuestas le permitirán al investigador

- Desarrollar un trabajo real y efectivo.
- Agradecemos su colaboración

Tabla No. 3.5: Administradores de Red y Laboratoristas

PREGUNTA	SI	NO
¿Existe políticas, normas y protocolos que regulen y aseguren la transmisión de los datos?		
¿Qué tipo de protocolos se encuentran instalados en su red?		
¿Cuáles de estos son utilizados en la Transmisión de VoIP?		
¿Qué tipos de códecs son utilizados en conjunto con los protocolos, para mejorar la calidad y su seguridad?		
¿Sabe de este tipo de transmisiones de VoIP sobre la red de la facultad?		
¿Con que frecuencia es analizada la seguridad de transmisión de datos en la red de la facultad?		
¿Se ha analizado la posibilidad de que este tipo de comunicación (VoIP) sature el canal de comunicación?		
¿Los protocolos implementados ayudan de manera eficiente en la transmisión de los datos?		
¿La comunicación entre emisor y receptor es óptima en todo momento?		
¿El modo de acceso al medio que utilizan los protocolos es el más recomendado?		

¿Existe un procedimiento de cifrado de las comunicaciones?		
¿Considera Usted que los protocolos utilizados en su red son los más eficientes?		
¿Piensa Usted que los protocolos utilizados en su red son los más óptimos?		
¿Considera Usted que los protocolos utilizados en su red tienen todo lo que necesitan para garantizar la seguridad en la red?		

ENTREVISTA AL ADMINISTRADOR DE REDES

LABORATORIOS E INSTALACIONES PARA DESARROLLO DE INVESTIGACIÓN

Tabla No. 3.6: Entrevista al Administrador de Redes

N° Pregunta	Pregunta	Respuesta
1	Cantidad de Servidores bajo su Administración, y con qué Funciones.	1 Servidor de Internet. 1 Servidor de Archivos. 1 Servidor para de gestión de red.
2	Marcas, Sistemas Operativos de los Servidores.	1 Compac Proliant 2 HP Proliant
3	Existen Routers, Firewalls, PIX, ASA, o algún equipo de Capa 3 que interconecten las redes de computadores y proporcionen puertas de acceso a internet.	1 Switch de Capa 3
4	Que cantidad de switchs, marca y cantidad de puertos tiene para la capa de acceso tiene.	14 Switchs 3COM de 24 puertos- Capa2
5	Existe algún método de seguridad o calidad de servicio en la red.	Creación de VLANs para cada laboratorio, MACs por puerto
6	Cuantas Ambientes, Laboratorios, tienen conectividad.	Existen 8 ambientes

CAPITULO IV

Análisis e Interpretación de Resultados

Modelo Analítico

Dentro del modelo analítico se analizan las topologías bases del prototipo de simulación que podrían ayudar en una futura implementación. Dentro de la variedad de las topologías existentes las analizadas son la topología tipo Estrella y Celda, ya que son las más utilizadas y que son con las que cuenta Facultad.

Topologías

Topología tipo estrella

La topología tipo estrella tiene la principal característica que tiene un nodo principal el cual si llega a fallar la red deja de funcionar. La ventaja de esta topología es que si se daña otro nodo, la red sigue funcionando. Además la fácil capacidad de expansión la hace una de las redes más usadas. Su principal desventaja es que al dañarse el nodo principal todos los nodos que están conectados no pueden comunicarse

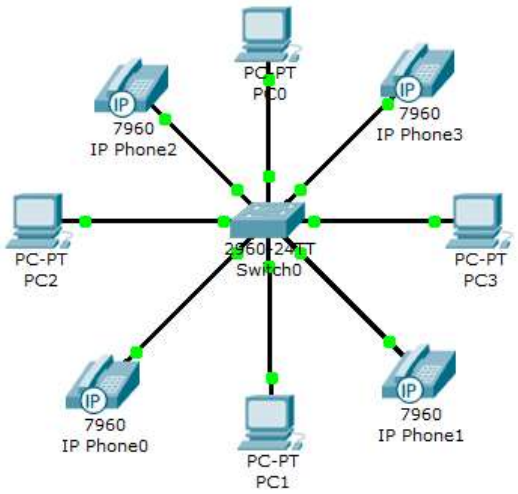


Figura No. 4.1: Topología Tipo Estrella
Elaborado por: Freddy Robalino

Topología celda o celular

La topología tipo celda o celular es usada para redes inalámbricas ya que está compuesta por áreas circulares o hexagonales, cada una de las cuales consta de un nodo individual. En este tipo de topología no hay enlaces físicos.

Otra aplicación es para unir áreas geográficamente distantes. La principal ventaja es que no se necesita de mayor instalación. La desventaja es que la señal está por todos lados y esto causa fallas por ruido y problemas de seguridad.

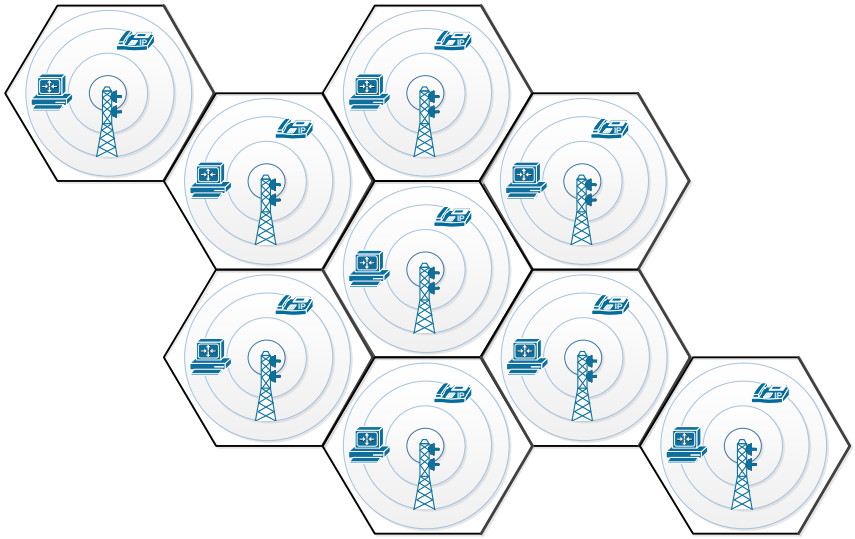


Figura No. 4.2: Topología Tipo Celular o Celda
Diseñado por: Freddy Robalino

Red Lan

Una vez definidas las topologías que se van a utilizar para el análisis de los protocolos, se muestra a continuación el diseño de las redes inalámbricas para los protocolos SIP y H.323 respectivamente

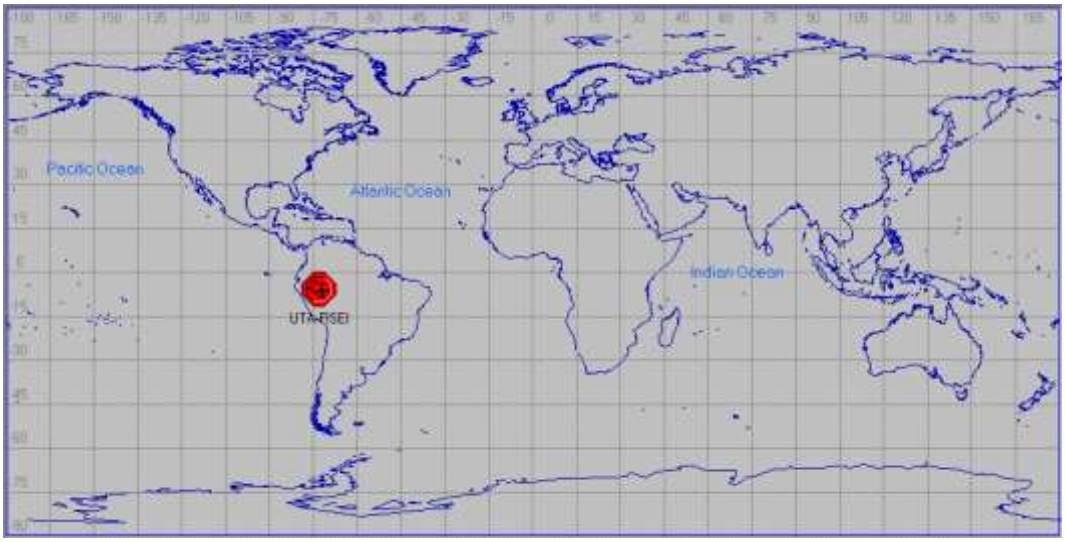


Figura No. 4.3: Ubicación Geográfica de la Red
Elaborado por: Freddy Robalino

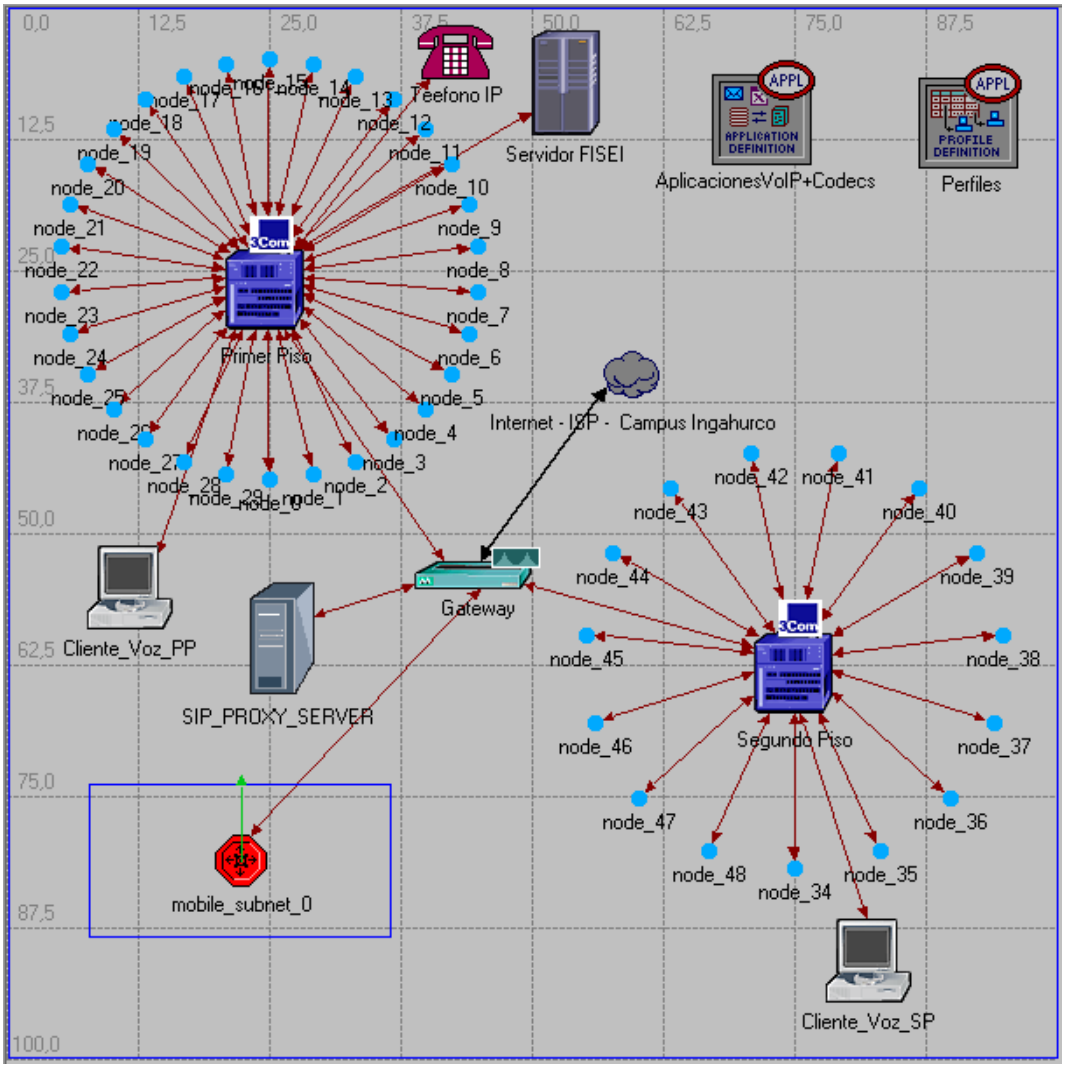


Figura No. 4.4: Topología de Red con SIP
Elaborado por: Freddy Robalino

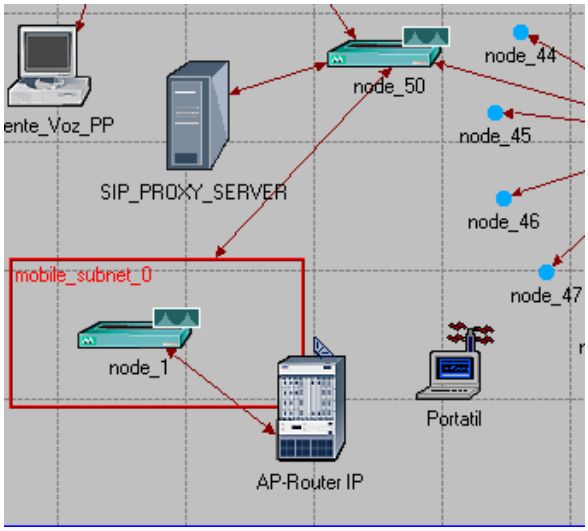


Figura No. 4.5: Interior del Nodo Wireless

En este diseño el manejo del flujo de paquetes está mejor balanceado. Las llamadas son las mismas para todos los diseños.

Se realizan del Piso 1 al Piso 2, de igual manera del Piso 2 al Piso 1. De esta manera todos son caller y called a la vez. Todos realizan y reciben peticiones para negociar la llamada. El servidor Proxy SIP está ubicado en el switch a donde acceden las subredes ayuda a la negociación y agilita él envió de paquetes.

En este diseño de red sólo existe un servidor Proxy y todos los paquetes tienen que pasar por un único Gateway. El servidor está ubicado próximo al Gateway, así se acelera las peticiones de todos los clientes.

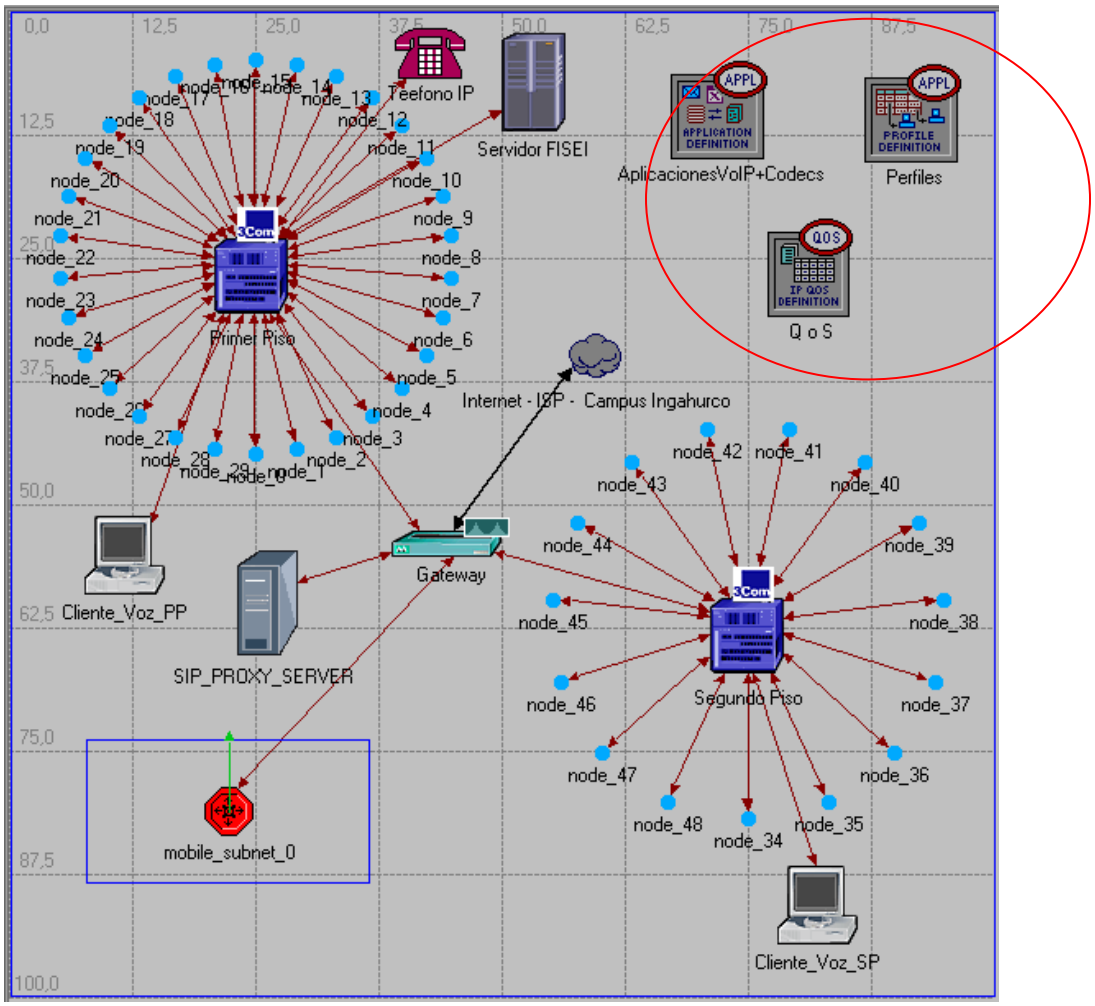


Figura No. 4.6: Topología de Red con H.323

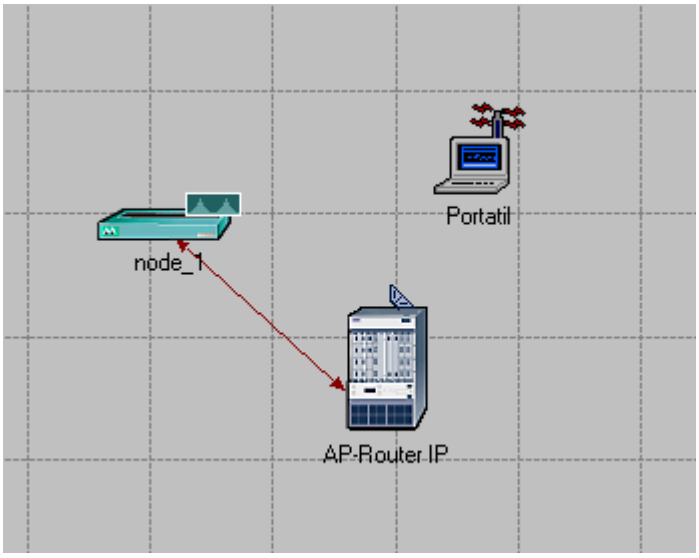


Figura No. 4.7: Interior del Nodo Wireless
Elaborado por: Freddy Robalino

Para el protocolo H.323 este diseño hace que la negociación para cada cliente tome más tiempo, debido a que se concentran en un solo nodo él envió de los paquetes.

Metodología

Parámetros a Evaluar

Se seleccionó de una lista de posibles parámetros que tienen mayor incidencia para determinar la calidad y aceptabilidad de la voz de un cliente a otro a través de una red Lan. Estos parámetros se los recolectó después de un estudio donde se recomienda los que se menciona continuación.

Jitter (variación del rendimiento)

En voz sobre IP el jitter es la variación de tiempo que hay entre los paquetes que llegan a su destino, es decir el tiempo que hay entre cada paquete al momento de su arribo.
Esto es causado por la cogestión en la red y por rutas alternas a la hora de enviar paquetes. Se aconseja que el valor del jitter sea lo más bajo posible. Para corregir el efecto de un jitter elevado se puede implementar el jitter buffer que ayuda a compartir un área donde los paquetes de voz pueden ser colectados, mantenidos y enviados.

Delay (Retraso - Demora)

Delay es el retraso o demora que hay entre la salida del paquete de voz hasta que llega a su destino, este parámetro está sujeto directamente a la cogestión de la red

Load (Carga)

El load se refiere a la carga que tiene una red. Es decir, la cantidad de información viaja a través de ella y cuántos paquetes puede manejar.

Tiempo de Señalización

Se define al tiempo de señalización al tiempo que se demora en establecer y autorizar el envío de paquetes de voz entre el que llama y el que va a recibir la llamada. Es decir, establecer y acordar todos los parámetros requeridos para la transmisión.

Envío y Recepción de Transferencia de Datos

Este parámetro se divide en dos: el tiempo de envió de los bits enviados (en segundos) y el tiempo de recepción de los (bits en segundo). Este parámetro indica cual es el porcentaje de bits perdidos durante la llamada y qué tan confiable puede ser.

Parámetros a variar

Para poder evaluar y decidir que parámetros son los que tienen mayor incidencia. Los parámetros a evaluar son:

Códec

Codec es una abreviatura de Compresor-Descompresor. Se puede implementar por software, hardware o una combinación de ambas, los códecs codifican una trama de una señal de datos a ser transmitida. Para poder recuperar los datos, hay que decodificar los mismos. La mayoría de los códecs provocan pérdidas de datos, esto es debido a que se busca tener el tamaño del paquete lo más pequeño posible. Algunos códecs aumentan el tamaño de la trama para evitar la pérdida de datos.

Los archivos multimedia contienen datos de audio, video y una referencia de cómo sincronizar el audio con el video.

Estos tres flujos hay que tener en cuenta para almacenar o transmitir y deben ser almacenados juntos, esto es lo que se conoce como formato de audio y video, mp3, mpg, avi, etc. Algunos de estos formatos son combinaciones de varios códecs.

Tabla No. 4.1: Especificación de códecs.

CODEC	Velocidad (Kbps)	Segmentos (bits)	Segmentos / s	Duración (ms)	Delay (ms)
G.711 (PCM)	64	8	8000	0.125	0.125
G.721 (ADPCM)	32	4	8000	0.125	0.125
G.723 (ADPCM)	24 – 40	3 -5	8000	0.125	0.125
G.726 (ADPCM)	16-64	2 – 8	8000	0.125	0.125
G.729 (CS-ACELP)	8	80	100	10	15
G.727 (ADPCM)	16-64	2 - 8	8000	0.125	0.125
G.728 (LD-CELP)	16	10	1600	0.625	0.625
G.723.1	6.3	189	33.33	30	37.5
G.723.1	5.3	159	33.33	30	37.5

Elaborado por: Freddy Robalino

Tipo de Señalización

Dentro de los parámetros a evaluar se encuentra el tipo de señalización.

Los tipos de señalización son:

Para el protocolo SIP, es “Call setup”, para el protocolo H.323, se implementa el protocolo RSVP como protocolo de señalización.

Voice Frame per Packets (VFPP)

El Voice Frame per Packets es el número de paquetes o tramas que van a ser agrupados para ser codificados antes de ser enviados.

ToS

Type of Service (ToS), el tipo de servicio que va a ser implementado en el sistema VoIP. El ToS provee un indicador de los parámetros de la calidad de servicio que se desea. Estos parámetros son usados para definir la calidad de servicio a la hora de transmitir el datagrama a través de la red. Algunas redes no admiten paquetes a menos que tengan cierto tipo de servicio.
La cabecera del datagrama del protocolo de Internet (IP) contiene un campo de 8 bits que es el destinado para definir el ToS.

- Bits del 0 al 2: Precedencia
- Bit 3: 0 = Retardo Normal, 1 = Retardo Lento
- Bit 4: 0 = Rendimiento Normal, 1 Rendimiento Alto
- Bit 5: 0 = Confiabilidad Normal, 1 = Confiabilidad Alta
- Bits del 6 al 7: Reservados para usos futuros

El uso del retardo, rendimiento y confiabilidad pueden incrementar el costo del servicio.

QoS

Quality of Service (QoS), se refiere a la calidad de servicio a la hora de transmisión de datos mediante el uso de control y medición del rendimiento y errores. QoS se refiere a la habilidad de una red de proveer

una mejor confiabilidad para seleccionar el tráfico de la red sobre varias tecnologías incluyendo redes ruteadas por el protocolo IP.

Al principio el QoS no era tan indispensable ya que los datos que se enviaban no necesitaban que lleguen en tiempo real y los usuarios no percibían la latencia de los datos. Con la implementación de redes inalámbricas y él envió de paquetes multimedia el uso de QoS se ha vuelto indispensable.

La demanda de los usuarios en la percepción del tiempo en las aplicaciones de voz y video en entornos inalámbricos hacen que surjan requerimientos en las aplicaciones tradicionales como la tolerancia mínima de retardo en la entrega de los paquetes y la intolerancia de la perdida de paquetes el jitter.

Número de Nodos

El parámetro número de nodos se refiere a la cantidad de clientes que se van a ir agregando en la red lógica que se planteará más adelante. Este parámetro es muy importante ya que se a mayor número de nodos que soporte los protocolos, estos serán más escalables.

Tipos de Simuladores

Dentro de los tipos de simuladores que podemos encontrar los más recomendados para nuestro propósito son el OPNET y el NS2

OPNET vs NS2

NS2 es un simulador que permite configurar varios parámetros, y aunque es muy recomendado, la gran desventaja que se presenta a la hora de utilizar NS2 es lo complicado de su interface y lo poco intuitivo para su manejo. OPNET es un simulador que fue desarrollado para poder simular y cubrir las mayores

necesidades dentro de una red y por ver los problemas que se presentan o prevenir una mala configuración de una red. La mayor ventaja de
OPNET es que es intuitiva su configuración. Su mayor desventaja es que permite configurar tantos parámetros que su configuración tiende a ser un poco tediosa, pero útil.

En este proyecto se usó la versión estudiantil de OPNET que es IT-GURU, el cual tiene algunas limitantes como el número máximo de eventos (500000) y la falta de módulos de red más avanzados. Para mayor detalle Ver (Anexo A)

OPNET – IT GURÚ

Modelos

Modelo de la topología.

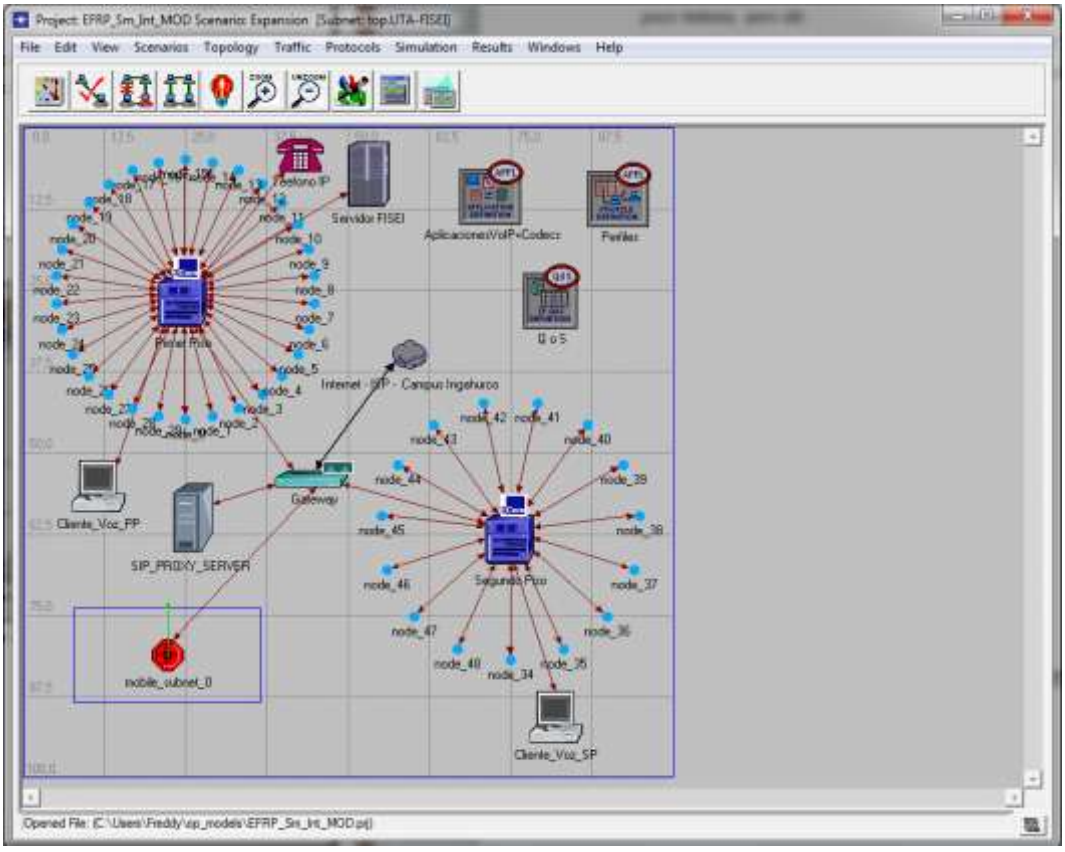


Figura No. 4.8: Modelo Analítico
Elaborado por: Freddy Robalino

Datos de Entrada

Los datos de entrada son los rangos de valores que van a ser variados en la simulación.
Dentro de los datos de entrada hay un valor que no se va a variar es solo para evaluar el rendimiento con VPN y sin VPN. El valor introducido son de los algoritmos de encriptación y de autentificación

Tabla No. 4.2: Datos Insertados en la Simulación para evaluar

Nombre	**Valor**
Códec	G.711 (PCM), G.729, G.723.1, GSM, G.726 (ADPCM), G.728 (LD-CELP), G.729 (CSACELP)
VFPP	1,2,3,7,10
ToS	Best Effort, Background, Standard, Excellent Effort, Streaming Multimedia, Interactive Voice, Reserved
QoS	FIFO, WFQ, Priority Queuing, Custom Queuing, MWRR, DWRR, MDRR
Nodos	3, 6, 12
VPN	0.0008 (seg)

Elaborado por: Freddy Robalino

Datos de Salida

Los datos de salida vienen dados en segundos, bytes por segundos y paquetes por segundo.

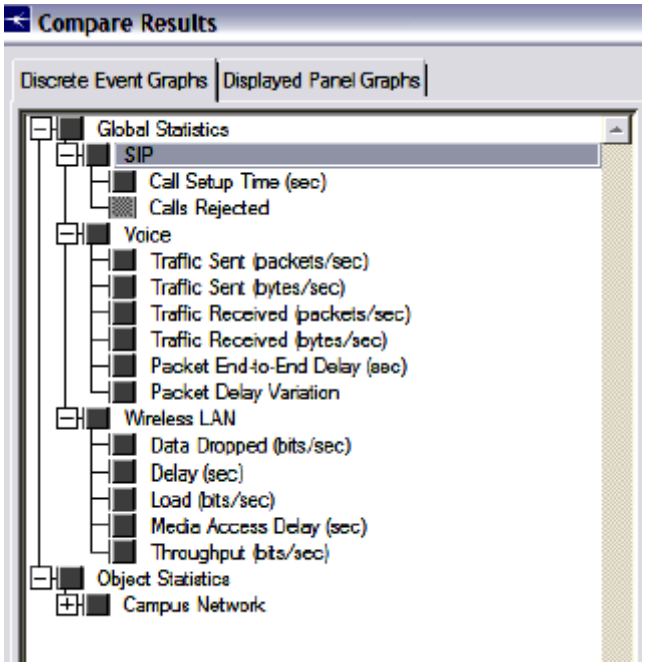


Figura No. 4.9: Selección de datos
Elaborado por: Freddy Robalino

Se puede escoger resultados de forma individual para cada nodo o de forma general para toda la red.

Configuración del Modelo Analítico

La configuración de los protocolos SIP y H.323 para el diseño del modelo de la topología es:

Protocolo SIP

Los parámetros a configurar en la definición de aplicación del modelo de la topología es:

Tabla No. 4.3: Configuración de los parámetros de voz para SIP

Atributo	Valor
Silence Length (seconds)	Default
Talk Spurt Length (seconds)	Default
Symbolic Destination Name	Voice Destination
Encoder	G.711
Voice Frames per Packets	1
Type of Service	Best Effort (0)
RSVP Parameters	None
Traffic Mix (%)	All Discrete
Signaling	SIP

Elaborado por: Freddy Robalino

La configuración en los terminales finales que van a realizar las llamadas y recibirlas es:

Tabla No. 4.4: Configuración de los parámetros de voz en el Cliente.

Atributo	Valor
UAC Service	Enabled
Proxy Server Specification	(...)
Máximum Simultaneous Calls	Unlimited
Proxy Server Connect (Seconds)	TCP Based

Elaborado por: Freddy Robalino

En el parámetro Proxy Server hay que agregar cuál es el servidor Proxy con el cual se va a comunicar el cliente para realizar la llamada.

En el servidor Proxy SIP hay que habilitar la opción de que se pueda aceptar las peticiones SIP.

Tabla No. 4.5: Habilitar el servidor Proxy.

Atributo	Valor
Proxy Service	Enable
Máximum Simultáneos Calls	Unlimited

Elaborado por: Freddy Robalino

Protocolo H.323.

Para el protocolo H.323 igual que para el protocolo SIP estas configuraciones se mantienen en la topología, la configuración en el modelo del simulador OPNET en su versión estudiantil es:
Configuración de la Definición de la Aplicación.

Tabla No. 4.6: Configuración de los parámetros de voz para H.323

Atributo	Valor
Silence Length (seconds)	Default
Talk Spurt Length (Seconds)	Default
Symbolic Destination Name	Voice Destination
Encoder Écheme	G.711
Voice Frames per Packets	1
Type of Service	Best Effort (0)
RSVP Parameters	(...)
Traffic Mix (%)	All Discrete
Signaling	None

Elaborado por: Freddy Robalino

La configuración del protocolo de reservación RSVP se configura por defecto. A esto se le agrega el tipo de calidad de servicio en los modelos donde se utiliza el protocolo H.323.
La configuración del cliente H.323 hay que tener en cuenta que hay que tener habilitado el tipo de señalización tanto en los clientes como en las interfaces de todo el recorrido hasta llegar al cliente que recibe la llamada, pasando por todos los nodos. Igualmente para el tipo de calidad de servicio.

Tabla No. 4.7: Activación del protocolo RSVP en las interfaces de los nodos

Name	RSVP Status	Máximum Reservable BW	Máximum Bandwich Per Flow	Subinterface Information
	Enable	**0,75**	**0,75**	**None**

Elaborado por: Freddy Robalino

Tabla No. 4.8: Habilitar el estatus del protocolo RSVP

Atributo	Valor
RSVP Status	Enable
Profile	Default

Elaborado por: Freddy Robalino

IPSec VPN

La configuraron del protocolo IPSec tanto para el protocolo H.323 y SIP es una parte importante de la simulación. Aunque esta parte se la realiza al final de la simulaciones. Para simular este parámetro se escogieron los valores de encriptación y autentificación para insertarlos durante la simulación.

Resultados

Los Resultados del modelo analítico en el simulador OPNET en su versión estudiantil son:

Códec

Topología con SIP

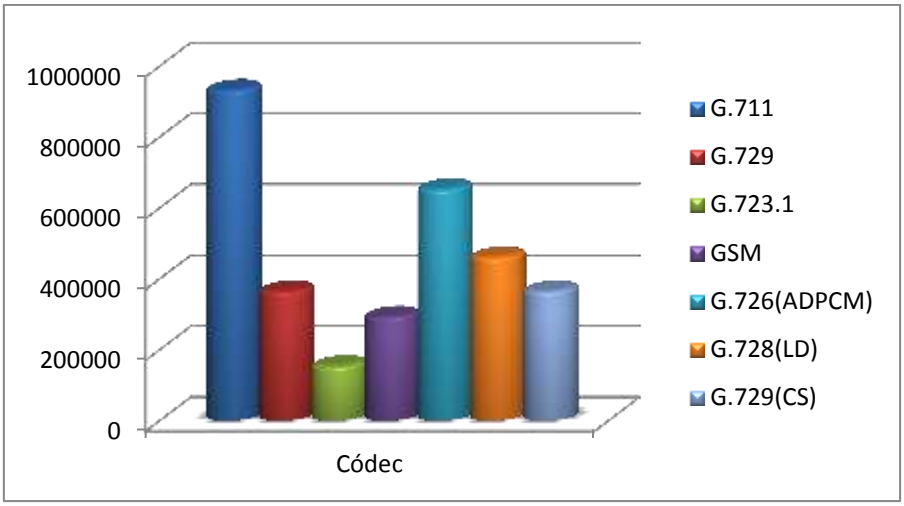


Figura No. 4.10: Diagrama codec de carga (SIP)
Elaborado por: Freddy Robalino

CÓDEC	Call Setup (seg)	Trafico Enviado (bytes)	Trafico Recibido (bytes)	Packet End to End Delay (seg)	Packets Delay Variation	Delay (Seg)	Load (bits/seg)
G.711(PCM)	0.024184	1500	927	2,709896406	0.4095024	1.3710195	932080
G.729	0.0115978	600	600	0.002244532	4,3112e-08	0.0008397	364800
G.723.1	0,015978	200	200	0,002336422	1,9218E-08	0,00083629	153600
GSM	0,015791	300	300	0,002797618	1,9975E-08	0,00100082	292800
G.726	0,017586	600	600	0,003087185	8,0847E-08	0,00110563	652890,6
G.728	0,017088	600	600	0,002755864	4,1452E-08	0,00104773	460800
G.729	0,016498	600	600	0,002244532	4,3112E-08	0,0008397	364800

Tabla No. 4.9: Resultados de la simulación de la topología SIP-CODEC

Topología con H.323

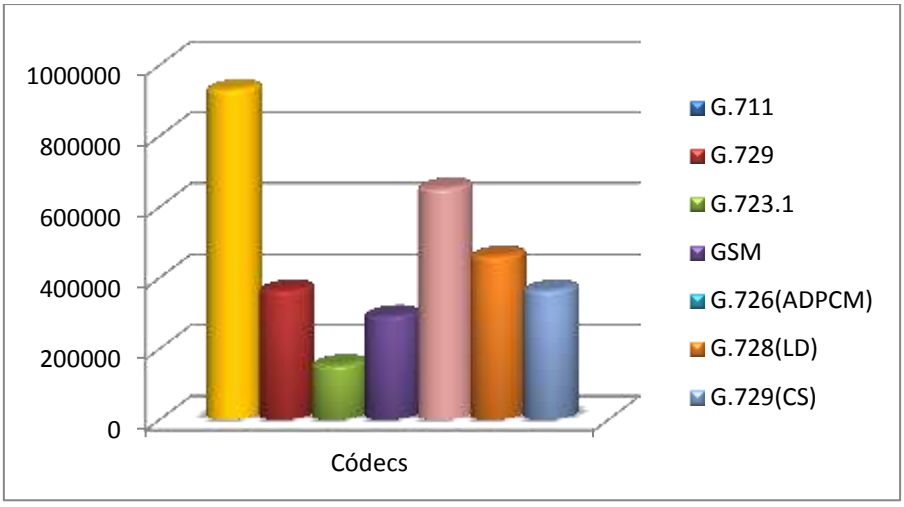


Figura No. 4.11: Diagrama codec de carga (H.323)
Elaborado por: Freddy Robalino

CÓDEC	Call Setup (seg)	Trafico Enviado (bytes)	Trafico Recibido (bytes)	Packet End to End Delay (seg)	Packets Delay Variation	Delay (Seg)	Load (bits/seg)
G.711	16,66666	1500	928,33	2,723129883	0.5706435	1.37028003	930400
G.729	16,66666	600	599,83	0.002258502	4,3272E-08	0.00084312	364800
G.723.1	16,66666	200	200	0,002673591	6,3725E-08	0,00098691	153600
GSM	16,66666	300	300	0,002715592	2,1178E-08	0,00094992	292800
G.726	16,66666	600	600	0,003624983	5,9927E-08	0,00135125	652890,6
G.728	16,66666	600	600	0,002809124	8,0544E-08	0,00106503	460736
G.729	16,66666	600	599,83	0,002258502	4,3272E-08	0,00084312	364800

Tabla No. 4.10: Resultados de la simulación de la topología H.323 - CODEC
Elaborado por: Freddy Robalino

Al variar el códec tanto para el protocolo SIP como H.323, nos muestran las Figuras 4.10 y 4.11 que el códec más adecuado es el G.711 (PCM) ya que a pesar de que tiene una menor compresión, esto conlleva a una calidad de voz mejorada, lo cual es una característica deseada en implementaciones de *VoIP Seguras*. Se escoge este códec ya que se quiere una mejor calidad en la voz transmitida. Además, como se evidencia en los datos obtenidos, la sobrecarga incurrida con el uso de G.711 no satura la red.

En el caso de desear sobrecargar menos la red (a un costo de calidad de voz reducida), se puede escoger otros de los códecs disponibles.

Señalización

Los resultados de la topología se evidencia que el protocolo SIP tiene menor tiempo para establecer la llamada. Esto debido a que el número de mensajes es menor comparado al protocolo H.323.

Voice Frame per Packets (VFPP)

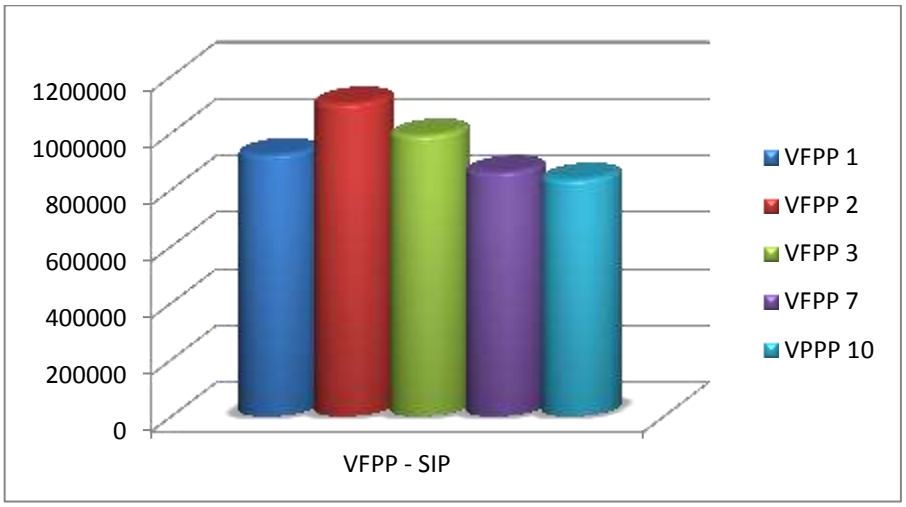


Figura No. 4.12: Diagrama VFPP de carga (SIP)

VFPP	Call Setup (seg)	Trafico Enviado (bytes)	Trafico Recibido (bytes)	Packet End to End Delay (seg)	Packets Delay Variation	Delay (Seg)	Load (bits/seg)
1	0,03074751	1500	925	2,724706965	0,738152294	1,3764471	923120
2	0.02784837	750	750	0,005026872	2,04956E-06	0,00199762	1103877,3
3	0,01663505	500	498,8888	0,005632561	1,31786E-06	0,00209367	991448,8
7	0,01663505	213,33	215,55	0,009730003	1,53619E-06	0,00347625	861280
10	0,01834965	150	150	0,012822593	2,32887E-06	0,00453347	835200

Tabla No. 4.11: Resultados de la simulación de la topología SIP – VFPP

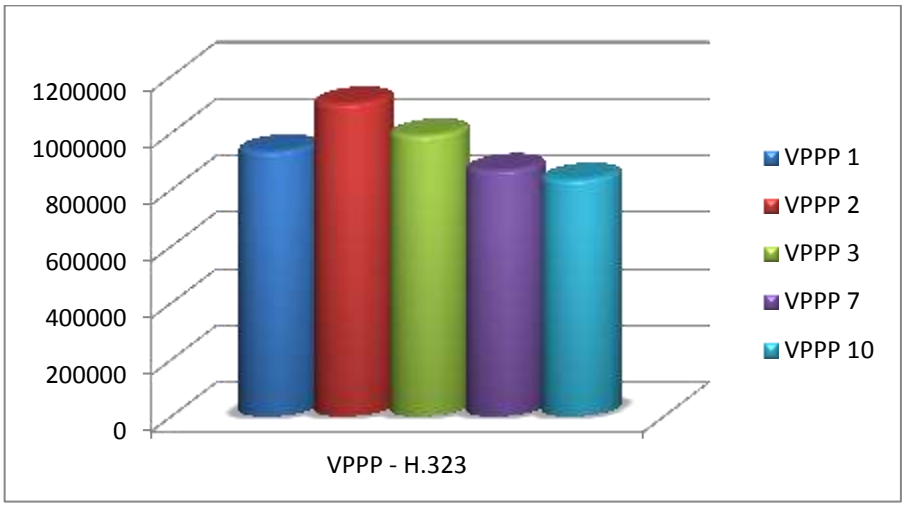


Figura No. 4.13: Diagrama VFPP de carga (H.323)

Elaborado por: Freddy Robalino

VFPP	Call Setup (seg)	Trafico Enviado (bytes)	Trafico Recibido (bytes)	Packet End to End Delay (seg)	Packets Delay Variation	Delay (Seg)	Load (bits/seg)
1	27,77777	1500	925	2,721532042	0,869542181	1,3690902	935733,33
2	27,77777	750	750	0,006104478	5,0521E-06	0,0024279	1104000
3	27,77777	500	498,8888	498,8888	0,66007733	2,7492E-06	992000
7	27,77777	213,33	213,3333	0,010020174	1,55948E-06	0,00347498	868000
10	27,77777	150	150	0,011036963	1,70332E-07	0,00360194	835200

Tabla No. 4.12: Resultados de la simulación de la topología H.323 - VFPP
Elaborado por: Freddy Robalino

El parámetro que se escogió para el VFPP es "2". Y se puede apreciar en las Figuras 4.12 y 4.13 que es el que más carga soporta. También se puede percibir que la variación de este parámetro afecta más al protocolo SIP.

Type of Service (ToS)

En la simulación que se realizó el ToS no varió mucho entre los protocolos; esto es debido a que el tráfico que se genero fue solo de voz. El parámetro que se escogió es el Interactive Voice debido a la característica del tráfico enviado para nuestra red.

Quality of Service

El resultado que se obtuvo con el QoS al variar los tipos de servicios no se obtuvieron grandes cambios debido a que este servicio se visualiza mejor con mayores cargas a las dispuestas para la red de la facultad.

Número de Nodos

Variación de la Carga

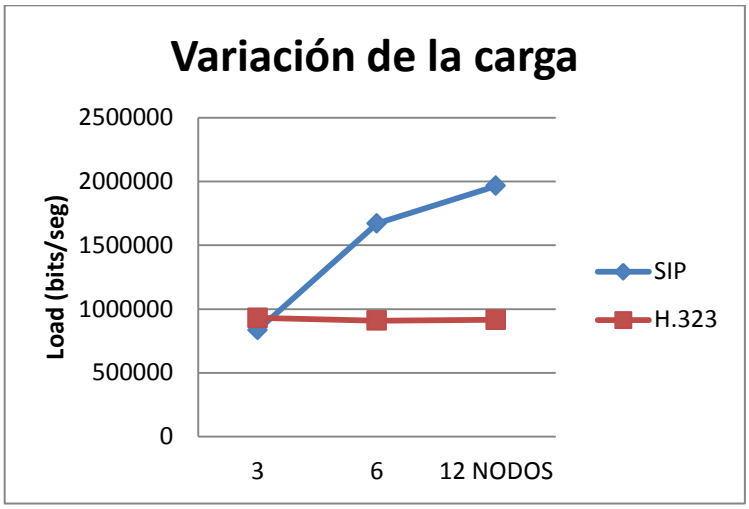


Figura No. 4.14: Cantidad de carga por nodo.

SIP							
NODOS	**Call Setup (seg)**	**Trafico Enviado (bytes)**	**Trafico Recibido (bytes)**	**Packet End to End Delay (seg)**	**Packets Delay Variation**	**Delay (Seg)**	**Load (bits/seg)**
3	0,02	1500	936,66	2,72	0,529739379	1,3717285	930666
6	11,24	1750	398,33	3,9	1,265127006	1,7237536	909866
12	31,44	2605	447,77	6,37	2,646151746	3,09550492	915466

Tabla No. 4.13: Resultados de la Variación de la carga por nodo (SIP)

H.323							
NODOS	**Call Setup (seg)**	**Trafico Enviado (bytes)**	**Trafico Recibido (bytes)**	**Packet End to End Delay (seg)**	**Packets Delay Variation**	**Delay (Seg)**	**Load (bits/seg)**
3	27,77	150	150	0,11390445	0.01141563	0,00377936	835200
6	55,55	300	299.44	0,016254715	0,016091104	0,00587609	1668853
12	114,44	600	188,88	2,309631476	1,46029866	1,46029866	1964266

Tabla No. 4.14: Resultados de la Variación de la carga por nodo (H.323).
Elaborado por: Freddy Robalino

Al incrementar los nodos se fueron configurando con los parámetros seleccionados en los resultados anteriores que mejor destacaron y se comparó con los diferentes protocolos.

Se puede valuar que para la topología implementada el ***protocolo SIP*** tiene un notable desempeño, incluso al incrementar los nodos que intervienen en la conversación su requerimiento de ancho de banda no es tan alto.
Por otro lado el protocolo H.323 a partir del nodo 3 se evidencia un incremento en uso de recursos también.

Entonces podemos llegar a la conclusión de que en la topología implementada aunque la carga se balancee mejor el protocolo H.323 no tiene un buen rendimiento. Aunque se podría utilizar con pocas estaciones no más de 4, y esto haría que el nivel de seguridad en la transmisión de datos seria débil.

VPN

El resultado de la simulación con el protocolo IPSec el cual es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores es definitivamente evaluar cuál es su desempeño frente a los protocolos H.323 y SIP. Dando buenos resultados.

El jitter es un parámetro más que nos permite ver el cambio o variación en cuanto a la cantidad de latencia entre paquetes de datos que se reciben y así poder ver el grado de seguridad en el trasporte de datos.

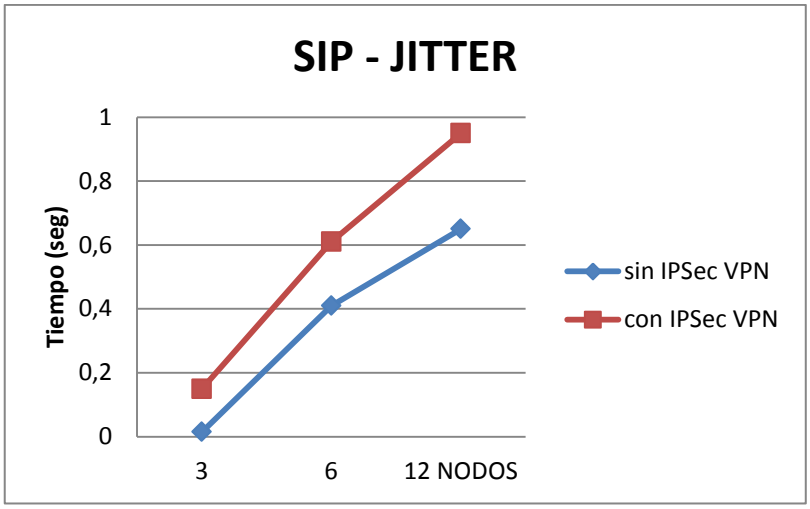


Figura No. 4.15: Variación del Jitter en una red VPN (SIP)
Elaborado por: Freddy Robalino

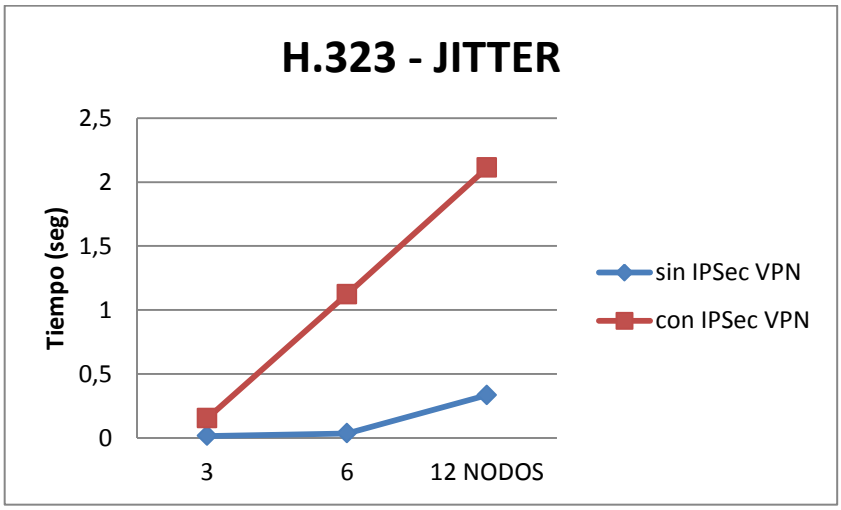


Figura No. 4.16: Variación del Jitter en una red VPN (H.323)
Elaborado por: Freddy Robalino

Al analizar los resultados conseguidos exponen que la variación del jitter es considerablemente alta para los dos protocolos. Debido a que el protocolo IPSec encripta los paquetes IP. Pero se puede visualizar que con el protocolo SIP el uso de IPSec en afecta menos el rendimiento.

Como conclusión podemos decir que la utilización del protocolo de seguridad IPSec incidirá en la seguridad de transmisión de los datos de una buena manera, aunque comprometa directamente al retardo de los paquetes.

Por tal motivo se recomienda el uso de este protocolo en zonas que no sean seguras.

Verificación de la Hipótesis:

Luego de haber tabulado y analizado todos los datos de las encuestas se ha escogido las preguntas más relevantes y de importancia para los cálculos de comprobación de las hipótesis planteada, para esto se ha optado la prueba de ji(chi-cuadrado) o X^2.

Para un detalle de los resultados y la tabulación de las encuestas ver la sección D.1 y D.2 del (ANEXO D).

La hipótesis a considerar es:

"Los protocolos de VoIP inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A."

- **Variable Independiente:** Protocolos de VoIP
- **Variable Dependiente:** Seguridad en la transmisión de datos.

1. Planteamiento de la hipótesis

   a. Modelo lógico

Hipótesis Nula Ho:

H_0: Los protocolos de VoIP SÍ inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A.

Hipótesis Alterna Hi:

Hi: Los protocolos de VoIP NO inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la

Prueba de $X^{2:}$

Protocolos de voz sobre IP incide en la seguridad de la transmisión de datos frente a la no incidencia de protocolos en la seguridad.

b. Modelo matemático

Donde las frecuencias observadas (***fo***) fueron relacionadas con los valores del Tráfico de voz sobre IP sin protocolos seguros y las frecuencias esperadas (***fe***) fueron las relacionadas con los valores de tráfico de voz sobre IP aplicando protocolos seguros.

H_0: $fo = fe$

Hi: $fo \neq fe$

c. Modelo estadístico

$$x^2 = \sum\left[\frac{(fo-fe)^2}{fe}\right]$$

2. Nivel de significación

El ***nivel de significación*** con el que se trabajó en la prueba de la hipótesis, fue de $\alpha = 0{,}05$. Por lo cual, la comprobación de cada resultado se comparó entre el valor de X^2 calculado, con el que se encuentra analizado en la tabla de Distribución de Chi Cuadrado

3. Zona de rechazo

Posterior a ello, se construyó la Tabla de Aplicación de la fórmula de X^2, tomando a ***fo*** y ***fe*** como valores para su construcción. Estas variables fueron utilizadas para el cálculo de X^2 y para establecer si su valor es o no significativo. Además se determinó los grados de libertad Donde ***f*** es el número de filas de la tabla de contingencia y ***c*** el número de columnas.

aplicando la siguiente fórmula:

	Probabilidad de un valor superior - *Alfa* (α)				
Grados libertad	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19

Figura No. 4.15: Tabla parcial X2
Elaborado por: Freddy Robalino

Fig. Tabla de distribución ji-cuadrado (X^2).

Grados de Libertad

$Gl = (c - 1)(f - 1)$ $Gl = (2-1)(2-1)$

$Gl = 1$

Figura:

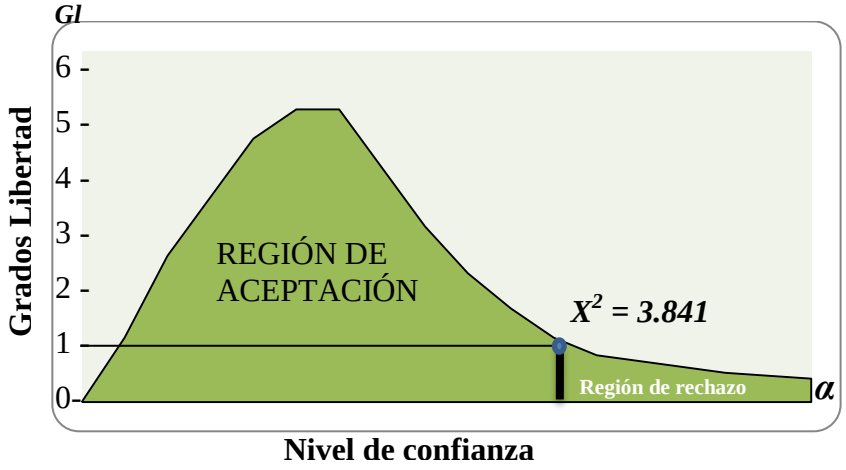


Figura No. 4.18: Campana de Gauss
Elaborado por: Freddy Robalino

4.- Análisis de Variables

ENCUESTA A ADMINISTRADORES DE REDES Y LABORATORISTAS

PREGUNTA	SI	NO
1.- ¿Existe normas y protocolos que regulen y aseguren la transmisión de los datos de VoIP?	0	100
2.- ¿Sabe de algunos protocolos de seguridad instalados en su red?	0	100
3.- ¿Los protocolos implementados actualmente ayudan de manera eficiente en la transmisión de los datos?	18.18	81.81
4.- ¿La comunicación entre emisor y receptor es óptima en todo momento?	18.18	81.81
5.- ¿El modo de acceso que utilizan los protocolos es el más recomendado?	18.18	81.81
6.- ¿Existe un procedimiento de cifrado de las comunicaciones?	18.18	81.81
7.- ¿Considera Usted que el protocolo utilizado en su red es eficiente?	27.27	72.72
8.- ¿Considera Usted que el protocolo utilizado en su red es el más óptimo?	27.27	72.72

Figura No. 4.15: Encuesta 1
Elaborado por: Freddy Robalino

Figura No. 4.19: Análisis grafico de datos E1-P1
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 11 personas encuestadas ósea el 100%, responde que no existen normas y protocolos que regulen y aseguren la transmisión de los datos de VoIP?

Figura No. 4.20: Análisis grafico de datos E1-P2
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 11 personas encuestadas ósea el 100%, responde que no conoce de algún protocolo de seguridad instalado en la red.

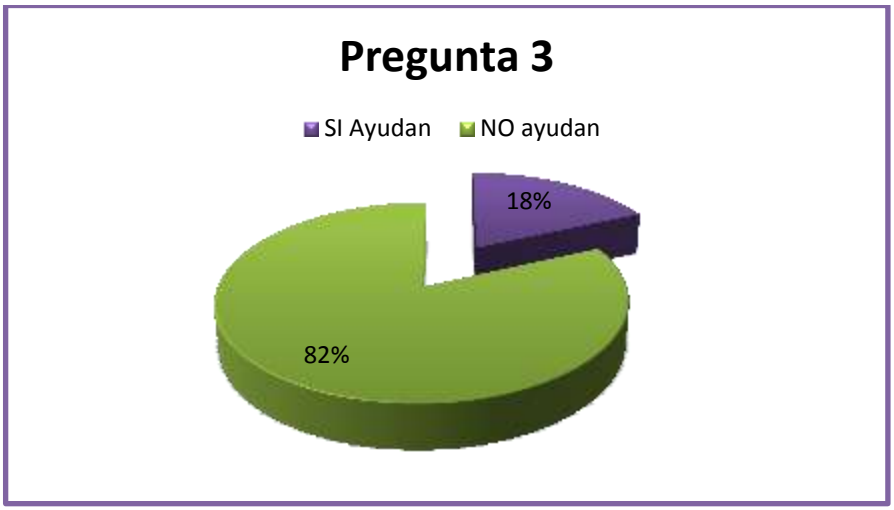


Figura No. 4.21: Análisis grafico de datos E1-P3
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde los protocolos implementados actualmente no ayudan de manera eficiente en la transmisión de los datos y el 18.18% dice que sí.

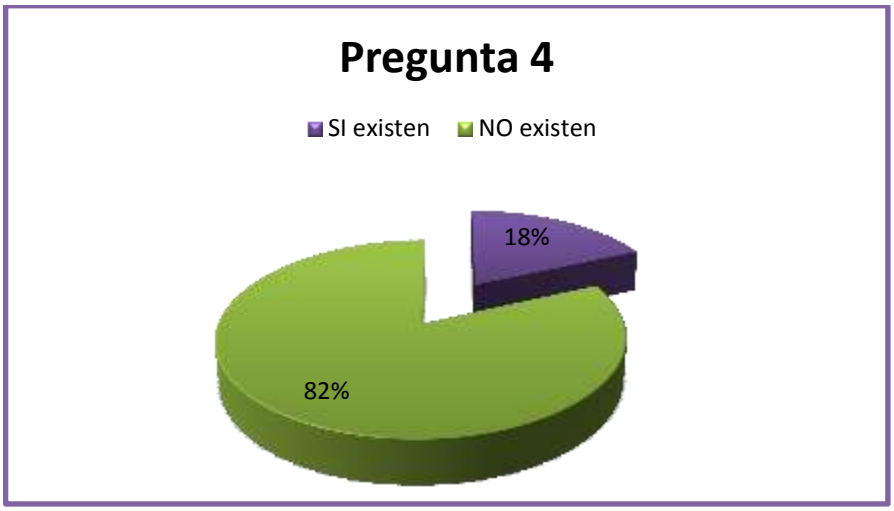


Figura No. 4.22: Análisis grafico de datos E1-P4
Elaborado por: Freddy Robalino

La comunicación entre emisor y receptor es óptima en todo momento

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que la comunicación entre emisor y receptor no es óptima en todo momento y el 18.18% dice que sí.

Figura No. 4.23: Análisis grafico de datos E1-P5
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que el modo de acceso que utilizan los protocolos no es el más recomendado y el 18.18% dice que sí.

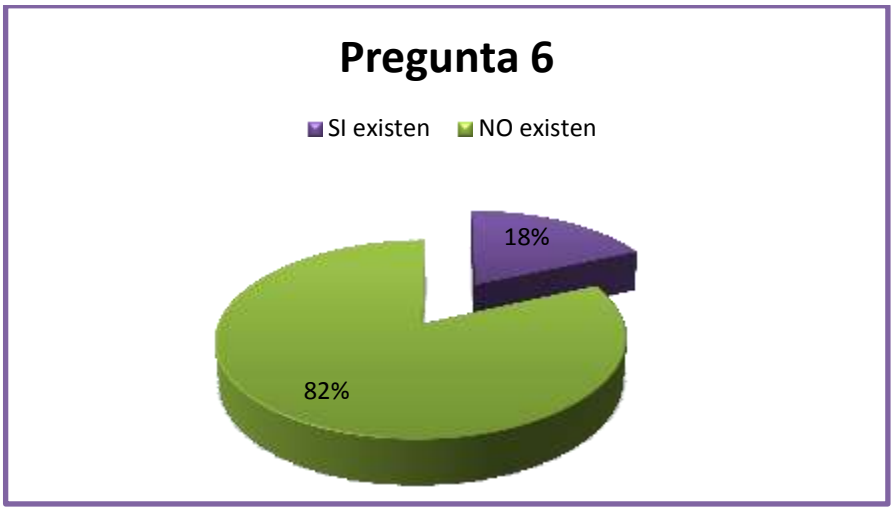


Figura No. 4.24: Análisis grafico de datos E1-P6
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que no existe un procedimiento de cifrado de las comunicaciones y el 18.18% dice que sí existe.

Figura No. 4.25: Análisis grafico de datos E1-P7
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que el protocolo utilizado en su red no es eficiente y el 18.18% dice que sí es eficiente.

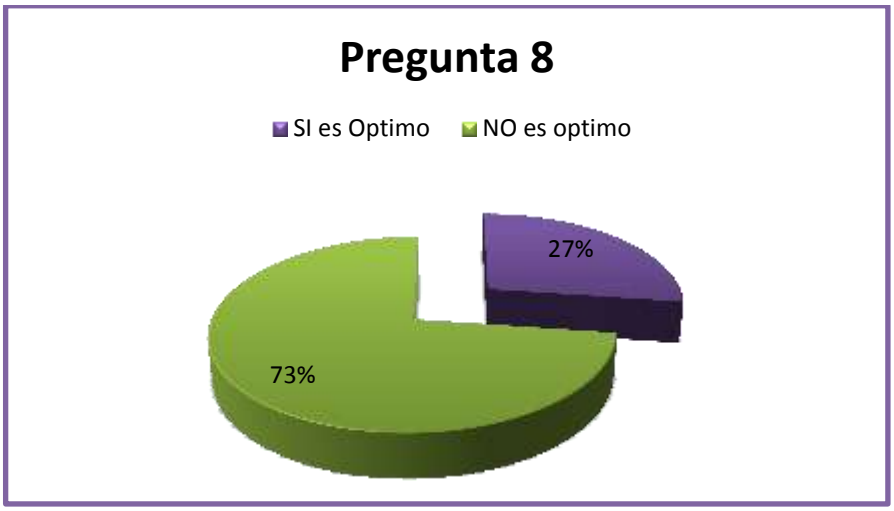


Figura No. 4.26: Análisis grafico de datos E1-P8
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que el protocolo utilizado en su red no es el más óptimo y el 18.18% dice que sí es.

ENCUESTA A DIRECTORES Y USUARIOS DEL SERVICIO Y LA RED

PREGUNTA	SI	NO
1.- ¿Ha tenido en cuenta la posibilidad de perder información, que se la roben, o que no sea correcta?	81.81	18.18
2.- ¿Existen controles que detecten posibles fallos en la seguridad?	18.18	81.81
3.- ¿Existen reglas que regulen la transmisión de voz en sus enlaces?	9.09	90.90
4.- ¿Utiliza algún método para priorizar el tráfico de las aplicaciones de voz?	0	100
5.- ¿La transmisión de datos es segura?	45.45	54.54

6.- ¿La transferencia y seguridad de datos en los enlaces de comunicación es eficiente?	36.36	63.63
7.- ¿La transferencia y seguridad de datos en los enlaces de comunicación es confiable?	45.45	54.54
8.- ¿Se dan seguridades a los datos?	18.18	81.81

Figura No. 4.16: Encuesta 2
Elaborado por: Freddy Robalino

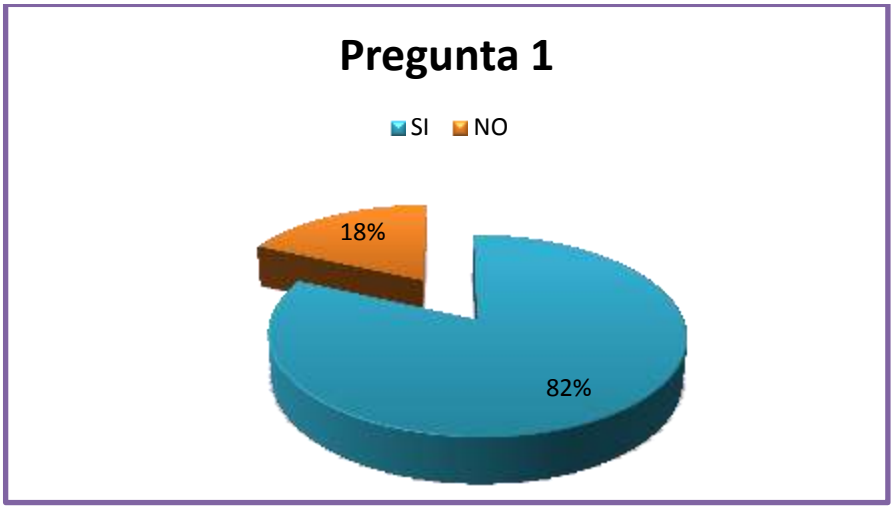


Figura No. 4.27: Análisis grafico de datos E2-P1
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que si se ha dado cuenta de la posibilidad de perder información, que se la roben, o que no sea correcta y el 18.18% dice que no.

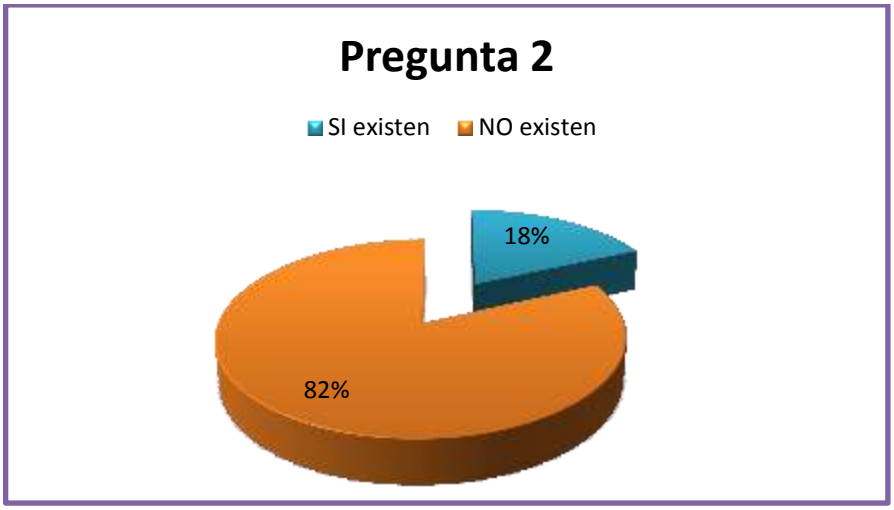


Figura No. 4.28: Análisis grafico de datos E2-P2
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que si existen controles que detecten posibles fallos en la seguridad y el 18.18% dice que no existen controles.

Figura No. 4.29: Análisis grafico de datos E2-P3
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 10 de las 11 personas encuestadas ósea el 90.9%, responde que no existen reglas que regulen la transmisión de voz en sus enlaces y el 9.09% dice que no existe regulación.

Figura No. 4.30: Análisis grafico de datos E2-P4
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 11 personas encuestadas ósea el 100%, responde que no existen métodos para priorizar el tráfico de las aplicaciones de voz.

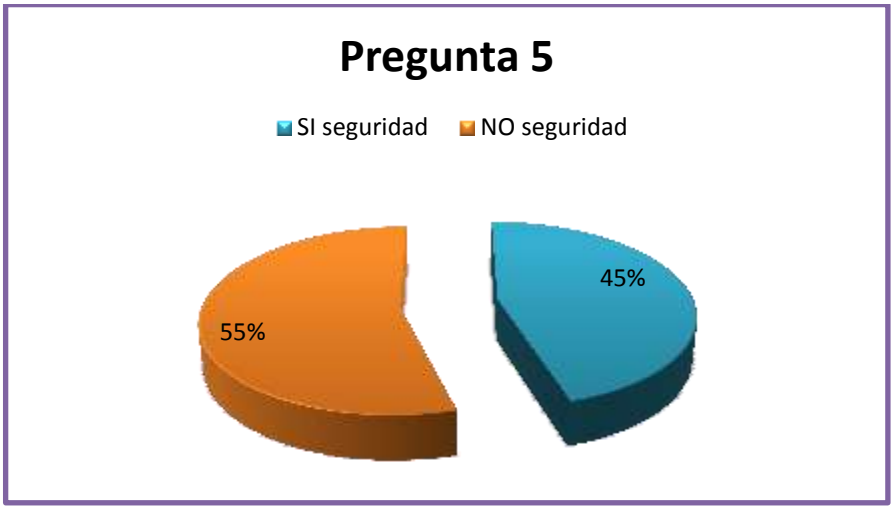


Figura No. 4.31: Análisis grafico de datos E2-P5
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 5 de las 11 personas encuestadas ósea el 45.45%, responde que la transmisión de datos si es segura y el 54.54% ósea 6 personas dice que no es segura.

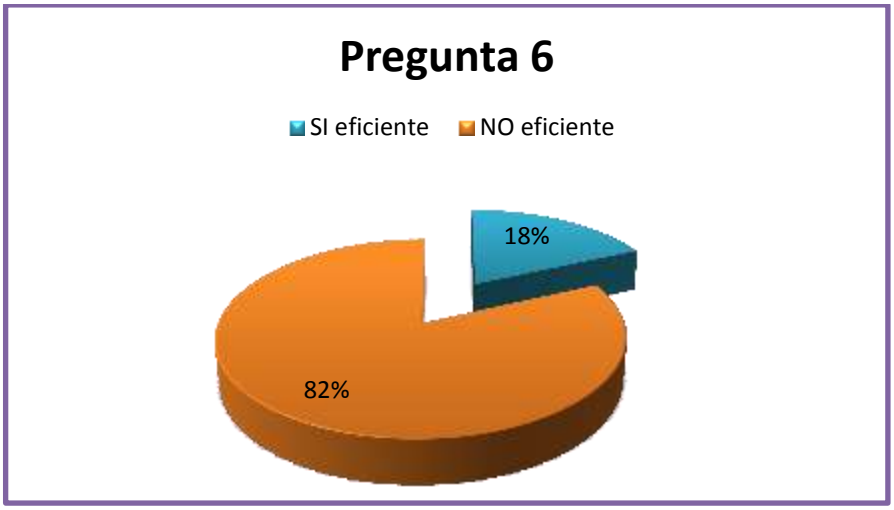


Figura No. 4.32: Análisis grafico de datos E2-P6
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 4 de las 11 personas encuestadas ósea el 36.364%, responde que la transferencia y seguridad de datos en los enlaces de comunicación si es eficiente y el 63.63% ósea 7 personas dice que no es eficiente.

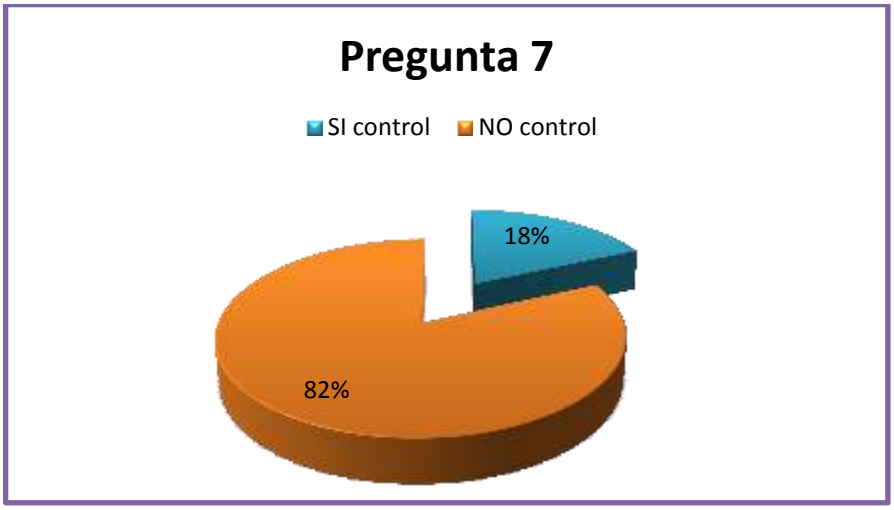


Figura No. 4.33: Análisis grafico de datos E2-P7
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que si existen controles que detecten posibles fallos en la seguridad y el 18.18% dice que no existen controles.

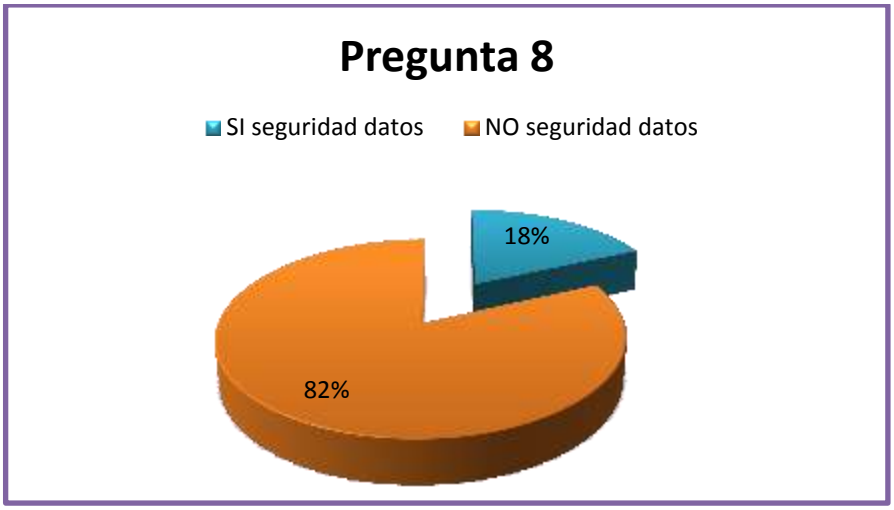


Figura No. 4.33: Análisis grafico de datos E2-P8
Elaborado por: Freddy Robalino

En esta pregunta podemos observar que las 9 de las 11 personas encuestadas ósea el 81.81%, responde que no se da seguridad a los datos y el 18.18% dice que si se da seguridad a los datos.

FRECUENCIAS OBSERVADAS

Protocolos de VoIP / **Seguridad en la transmisión de datos**	No Confiable	Confiable	TOTAL
No segura	2	2,5	4,5
Segura	9	8,5	17,5
TOTAL	11	11	22

Tabla No. 4.17: Análisis de Variables – Frecuencias Observadas.
Elaborado por: Freddy Robalino

Encuestas combinadas

Estos datos son tomados de las preguntas más relevantes e importantes de las dos encuestas.

FRECUENCIAS ESPERADAS

Protocolos de VoIP Seguridad en la transmisión de datos	No Confiable	Confiable	TOTAL
No segura	2,25	2,25	4,5
Segura	8,75	8,75	17,5
TOTAL	11	11	22

Tabla No. 4.18: Análisis de Variables – Frecuencias Esperadas.
Elaborado por: Freddy Robalino

Aquí podemos observar que ***fo*** = ***fe.***

4.- Cálculo de X^2

En la siguiente tabla se muestra las frecuencias observadas y esperadas de los indicadores, analizando si cumplieron o no con la hipótesis planteada, esto basado en la Prueba de Chi cuadrado. Cabe recordar que el cumplimiento de la hipótesis se da si el valor calculado es mayor al que se encuentra analizado (tabulado) en la tabla de Distribución de Chi Cuadrado en este caso X^2*=3.841(Tabla Completa-Ver Anexo F).*

fo	fe	fo - fe	(fo - fe)2	(fo - fe)2/ fe
2	2,25	-0,25	0,06	0,03
9	8,75	0,25	0,06	0,01
2,5	2,25	0,25	0,06	0,03
8,5	8,75	-0,25	0,06	0,01
TOTAL				0,07

Tabla No. 4.19: Análisis de Variables – Frecuencias Esperadas.
Elaborado por: Freddy Robalino

Decisión:

Con 1 grados de libertad y 95% de confiabilidad, aplicando la prueba X^2 (Chi-Cuadrada) se tiene que el valor tabular es igual a 3.841; de acuerdo a los

resultados obtenidos con los datos tomados de la encuesta se ha calculado el valor de X^2 que alcanza a 0.07; lo que implica que se acepta la hipótesis nula, que dice: Los protocolos de VoIP SÍ inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A.

De esta manera podemos decir que la falta de seguridad en la red de la facultad, se debe a los métodos utilizados para transportar y asegurar la información. Y el eslabón más débil de esta cadena son los protocolos de seguridad que no están implementados, y aún más conociendo que el medio más utilizado para la transmisión de este tipo datos no es la propia red si no que es la Internet, la cual no garantiza la seguridad de los mismos, por eso es importante disponer de protocolos seguros que ofrezcan métodos de cifrado como el uso de túneles IPSec para proteger el tráfico de VoIP.

CAPITULO V

Conclusiones y Recomendaciones

Conclusiones

Después de efectuada la presente investigación se concluye que:

- La Facultad de Ingeniería en Sistemas, Electrónica e Industrial no posee una infraestructura propia para VoIP, y por consecuencia no existen ningún protocolo específico implementado para VoIP en la red de la FISEI, y así dar seguridad a la transmisión de voz.

- Para poder realizar la investigación se necesitó implementar un prototipo con características similares a la de la red de la FISEI, pero trabajando sobre la base de los dos protocolos de VoIP más utilizados como son (SIP y H.323).

- Al variar los parámetros más significativos como (Códecs, VFPP, ToS, QoS, Nodos, VPN) en la topología, se pudo determinar el rendimiento y el nivel de seguridad que ofrecen los protocolos SIP y H.323 a transmisión de datos.

- El protocolo SIP se destacó por su alto rendimiento al combinar las diferentes variables, aunque H323 es un poco más seguro, pero SIP puede ser compensado con el protocolo IPSec para incrementar inmejorablemente su seguridad.

- El nivel de seguridad en la trasmisión de datos de la red también se ve afectada por el desconocimiento de métodos que aseguren el transporte de voz sobre ip.

- Tras la investigación se concluye que la mejor alternativa en cuanto a software de análisis, captura y emulación de tráfico de datos, ya que provee de muchos parámetros de configuración acercándose a la realidad lo más posible es el OPNET IT-GURU.

Recomendaciones

- Al implementar seguridad en los protocolos, hay que tener en cuenta que estos pueden afectar su latencia considerablemente.

- Tras los estudios realizados se recomienda los protocolos H.323 y SIP en servidores y clientes de código abierto.

- Utilizar protocolo SIP no solo por su sencillez en la configuración sino su estabilidad al aumentar los nodos que intervienen en la transmisión de voz.

- Tener en cuenta los aspectos más importantes para una correcta implementación de VoIP, como son la implementación de técnicas de Calidad de Servicios (QoS), seguridad y direccionamiento IP entre otros.

- La capacitación permanente del personal del departamento de redes y áreas afines debe ser siempre una prioridad.

- Se recomienda que se establezcan políticas de seguridad para la red de la facultad y la universidad debido a que se pudo determinar que los datos de VoIP viajan utilizando la red LAN de la universidad hasta salir a la WAN y nuevamente regresar a la misma para así evitar los huecos de seguridad.

- En el caso de tener acceso a la compra de una licencia se recomienda utilizar el simulador OPNET en su versión completa, para poder evaluar mayores tipos de seguridades y se pueden recoger muchas estadísticas de la red como la productividad (throughput) y el retardo de permanencia en cola del enlace WAN.

CAPITULO VI

LA PROPUESTA

TEMA:

DISEÑO DE UNA RED PRIVADA VIRTUAL (VPN) CON EL PROTOCOLO IPSec PARA BRINDAR SEGURIDAD A LA TRANSMISIÓN DE DATOS EN LA F.I.S.E.I. DE LA U.T.A.

Datos Informativos

Campo: Telecomunicaciones

Área: Redes

Institución: F.I.S.E.I. de la U.T.A.

Dirección: Campus Huachi - Av. Chasquis y Rio Payamino.
Campus Ingahurco - Av. Colombia entre Chile y Salvador.

Ciudad: Ambato

Antecedentes de la Propuesta

Las redes de hoy en día están evolucionando y permitiendo el transporte de datos, voz y video, tendiendo de esta forma redes convergentes. Actualmente, con los múltiples servicios sobre Internet y la necesidad de la F.I.S.E.I. de la U.T.A. de proteger y dar seguridad a sus comunicaciones, considerando que estas no tienen protocolos seguros para la transmisión de datos y adicional a esto la comunicación VoIP la hacen utilizando los enlaces con los proveedores de internet y de manera generalizada han optado el uso de Internet como un medio de transporte los cuales no proveen mayor protección, de comunicación entre sus oficinas o campus

remotos. Lo cual ha sido evidenciado en la investigación a través de los datos obtenidos, que los protocolos de VoIP utilizados si inciden en la seguridad de la trasmisión de los datos.

Todo esto crea la necesidad de diseñar una red privada virtual (VPN) con el protocolo de seguridad IPSec para proporcionar protección a los paquetes IP sobre la red. Esta combinación permitirá brindar la máxima seguridad y confidencialidad en la transmisión de los datos (voz), encriptándola para garantizar que la señal no sea interceptada por agentes externos a la red.

Cabe acotar que la FISEI cuenta con el proyecto aprobado para el 2011 de Diseño e Implementación de un sistema de comunicación de VoIP para la UTA utilizando el software libre Asterisk. Dicho proyecto fue desarrollado anteriormente con Elastix[17], A cargo del Ing. David Guevara M.Sc y el Ing. Eduardo Chaso.

Justificación

Después de realizar una investigación respecto a la incidencia de los protocolos en la seguridad de la trasmisión de datos VoIP, así como encuestas técnicas a profesionales en la rama y administradores de redes actuales y presentes, se concluyó que los protocolos seguros son un parámetro que si protege la transmisión y además no existe un método o forma garantizar que los datos de VoIP transmitidos en la Facultad y la Universidad lleguen seguros.

Actualmente en toda la Universidad y en nuestra Facultad, están interesados en aplicar tecnologías de VoIP seguras dentro de la institución, pero estas no cuenta con parámetros y pautas de seguridad de transmisión de información, lo cual hace más difícil la consecución de los objetivos finales, ya que además por desconocimiento se llega a casos de sub-dimensionamiento de los requerimientos de seguridad y compra de soluciones que no son las adecuadas a las necesidades de la institución. En otras ocasiones debido a que no se hace un análisis de requerimientos de red e institución en el momento, se hace necesario en este caso,

rediseñar la red de datos para poderla ajustar a las exigencias de seguridad de la misma y de los usuarios y administradores del servicio.

En la investigación se pudo observar que en ningún estamento de la facultad y la universidad se toman medidas de seguridad para la transmisión de datos VoIP.

Por las razones expuestas anteriormente y el hecho que toda la universidad se encuentre enlazada, recomiendo se aplique a toda la red, los parámetros de seguridad propuestos.

Además se exhorta a la entidad correspondiente se tome como guía el modelo planteado en este documento ya que les permitirá tener una orientación clara de que es lo que se quiere implementar y que cambios se deberán tener en cuenta dentro de la toda red de la institución para poder llevar a cabo la implementación de una solución segura para VoIP que satisfaga las necesidades y requerimientos de la institución.

En este documento se fijan los parámetros importantes a tener en cuenta para poder hacer la implementación del diseño propuesto, teniendo en cuenta posibles crecimientos y necesidades futuras de la solución y la red de datos.

Objetivos

Objetivo General

Diseñar una red privada virtual (VPN) con el protocolo IPSec, para brindar seguridad a la transmisión de datos VoIP en la F.I.S.E.I y la U.T.A.

Objetivos Específicos

- Proponer y diseñar una topología de red VPN utilizando protocolos de seguridad como IPSec, que proporcione conectividad segura a través de la LAN, WAN.

- Definir reglas técnicas de configuración para efectuar el túnel VPN con IPSec.
- Describir los pasos para establecer una sesión VPN Utilizando IPSec.
- Proponer un esquema de telefonía ip administrada con asterisk Now para la UTA.

Análisis de Factibilidad

Luego del estudio realizado se concluye que es factible la adaptación de una red privada virtual VPN con el protocolo IPSec, para brindar seguridad a la transmisión de datos VoIP en la red de la facultad, ya que la facultad cuenta con la infraestructura lógica y física además de una partida extra equipos.

Además se ha podido determinar qué el departamento de Administración de Redes tiene la capacidad técnica para ejecutar el proyecto. Se revisó el nivel de preparación del personal Técnico determinando que son Ingenieros en Sistemas o afines y que poseen cursos y/o certificaciones en Redes y manejo de LINUX.

En cuanto a los requerimientos de ancho de banda la universidad dispone de 28mb en la actualidad este ancho indicado cubre las necesidades para la implementación.

Los equipos existentes como los switchs 3COM pueden servir en la capa de acceso, además disponen de router Cisco Catalyst3750 que se puede reutilizar, para la comunicación.

Fundamentación

Elementos de seguridad IPSec

Introducción

El crecimiento acelerado de Internet, su conectividad, los usuarios y además de la de nuevos servicios como el de Voz sobre IP, han originado que intrusos técnicamente avanzados vean consideren como un reto el emprender diversos ataques que amenacen la integridad, confidencialidad, privacidad y la seguridad de redes de comunicación de datos en general.

En especial el temor a intrusos anónimos provenientes de Internet está obligando a las empresas u organizaciones a considerar soluciones radicales tales como la separación entre redes de datos privadas (Intranets-VPN) y la red pública Internet. La segmentación obtenida se está constituyendo en un fuerte impedimento para lograr el concepto de una red Internet global, lo que establecería una conectividad fuertemente acoplada.

En 1994, el IAB-Internet Architecture Borrad- emitió el reporte "Security in the Internet Architecture" (RFC 1636), el cual establecía que Internet requería una mayor y mejor seguridad, además, identificaba las áreas claves que requerían mecanismos de seguridad. Entre las principales necesidades quedaron identificadas: el aseguramiento de la infraestructura de red, tanto del monitoreo como del control del tráfico no autorizado, y la protección del trafico usuario a través de protocolos seguros de usuario a usuario además de utilizar mecanismos de autentificación y de encriptación (QoS).

El protocolo de Internet IP, es uno de los más utilizados para la interconexión de redes tanto en ambientes académicos como corporativos, y obviamente es también muy usado en la Internet pública. Su flexibilidad y sus poderosas capacidades lo han impuesto como un vehículo de interconectividad por un largo tiempo.

Sin embargo, IP presenta ciertas debilidades. Debido a la forma en que el protocolo enruta los paquetes, da como consecuencia que las grandes redes IP sean vulnerables a ciertos riesgos bien conocidos de seguridad.

De tal forma que si no se toman medidas de seguridad ni se aplican controles, los datos también pueden ser objeto de ataques externos. Estos pueden ser ataques pasivos (solo se observa la información), como ataques activos (se modifica la información con intención de dañar o destruir los datos o la propia red.)

Seguridad del protocolo internet (IPSec).

Debido a que los riesgos de los diferentes ataques complican el uso de las redes IP (incluyendo por supuesto a toda Internet) en comunicaciones altamente sensibles, un grupo internacional organizado bajo el IEFT desarrolló el IPSec, como un conjunto de extensiones para IP que ofrecen servicios de seguridad en el nivel de red (de acuerdo con el modelo de capas de ISO de OSI). La tecnología de IPSec se basa en la criptografía moderna, lo que garantiza, por un lado, la privacidad y, por otro, una autentificación fuerte de datos.

La Seguridad del Protocolo de Internet es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes con el Protocolo de Internet mediante el uso de servicios de seguridad criptográfica.

Este estándar es obligatorio para soluciones IPv6 para el cual fue definido, y ha sido adaptado para soluciones IPv4, en las que es optativo.

IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo

controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

Modos de operación de IPSec

Existen dos modos en los que opera IPsec, modo transporte y modo túnel:

Modo Transporte.

El modo transporte protege la carga útil del paquete IP, es decir en este modo IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec (AH) entre la cabecera IP y la cabecera
del protocolo de capas superiores.

En el modo transporte, el cifrado se realiza extremo a extremo, del host origen al host destino, y este modo es más confiable que el modo túnel.

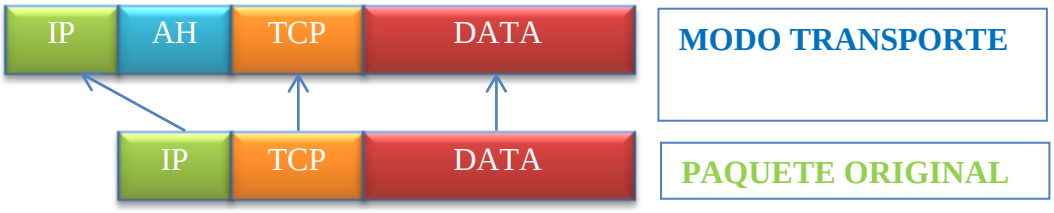


Figura No. 6.1: Modos de Transporte IPSec
Elaborado por: Freddy Robalino

Figura No. 6.2: Cifrado extremo a extremo

Modo Túnel

El modo túnel protege los paquetes IP completos. Es decir en este modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec.

En este modo la comunicación segura se limita a los routers de acceso implicados. Es el modo más usual en una VPN

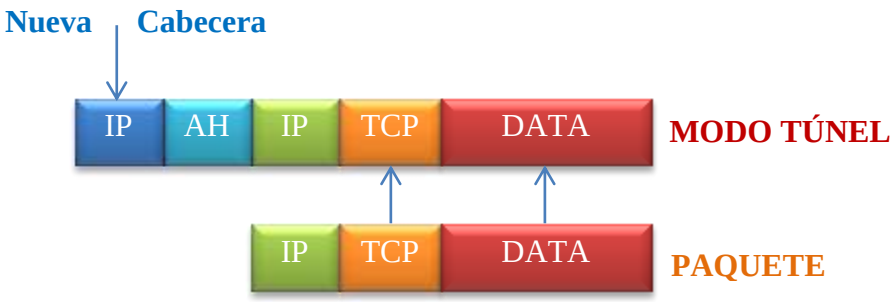


Figura No. 6.3: IPSec Modo Túnel
Elaborado por: Freddy Robalino

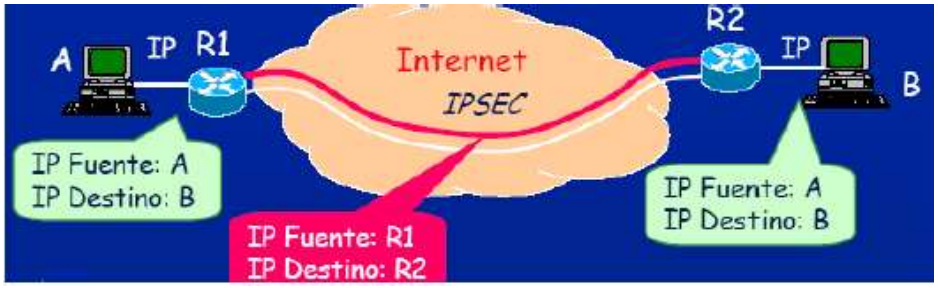


Figura No. 6.4: Comunicación segura limitada a los routers

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5- Message.

Digest Algorithm 5 - (Algoritmo de Resumen del Mensaje 5) y SHA- Secure **Hash Algorithm** - (Algoritmo de Hash Seguro) para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de los datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por rechazo de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

LOS PROTOCOLOS IPSEC

IPSec está formado por tres protocolos principales:

- Un protocolo de autenticación, referido como Cabecera de Autenticación (AH- Authentication Header-).
- Un protocolo combinado de autentificación/encriptamiento llamado Carga de Seguridad Encapsulada (ESP- Encapsulating Security Payload-).
- Un protocolo de intercambio de llaves, (IKE- Internet Key Exchange-).

Cabecera de Autenticación (AH)

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete. La cabecera AH mide 24 bytes.

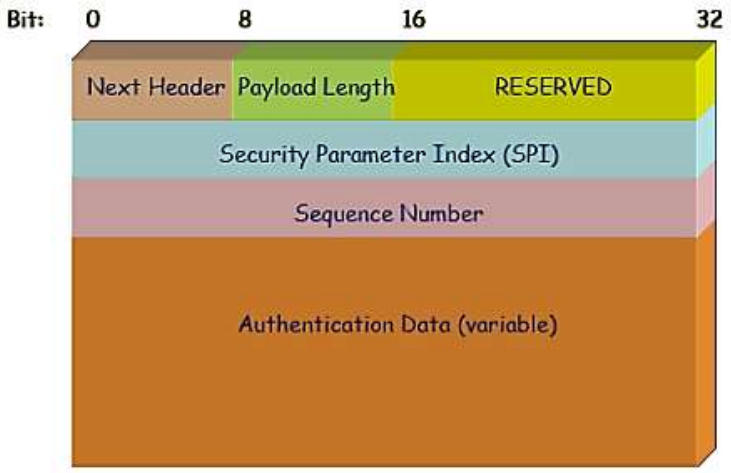


Figura No. 6.5: Cabecera de Autenticación (AH)

- El primer byte es el campo "Siguiente cabecera". Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6.
- El siguiente byte especifica la "longitud del contenido del paquete". Este campo está seguido de dos bytes reservados.
- Los siguientes 4 bytes especifican el "Índice de Parámetro de Seguridad (SPI)". El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete.
- Luego tenemos los siguientes 4 bytes que pertenecen al "Número de Secuencia" (32 bit), este número protege frente a ataques por repetición.
- Los últimos 12 bytes (96 bit) almacenan el "código de resumen para la autenticación de mensaje" (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Carga de Seguridad Encapsulada (ESP).

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes.

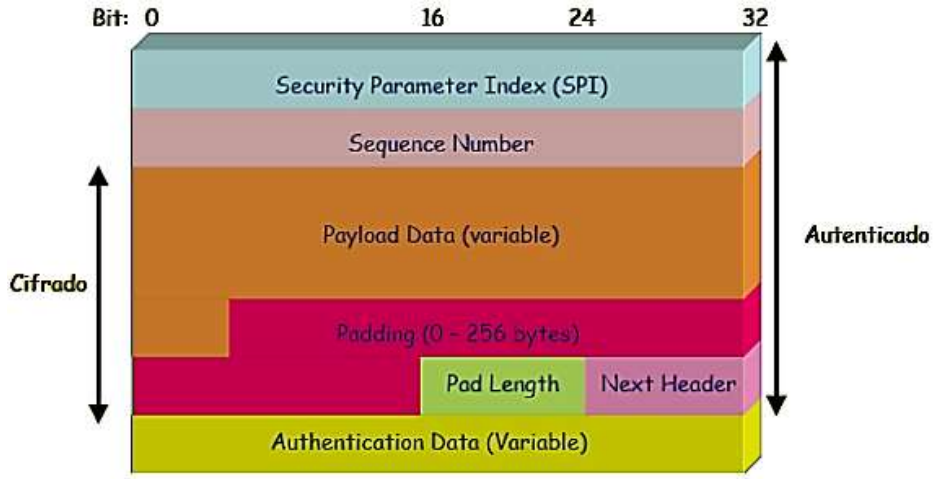


Figura No. 6.6: Carga de Seguridad Encapsulada - Protocolo (ESP)

- Los primeros 32 bits de la cabecera ESP especifican el "Índice de Parámetros de Seguridad (SPI)". Este SPI especifica qué SA emplear para desencapsular el paquete ESP.
- Los siguientes 32 bits almacenan el "Número de Secuencia". Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes.
- Los datos cifrados del protocolo IP están dentro del "Portador de datos" (Payload Data).
- IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario "rellenar (Padding)" la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la "longitud del relleno (pad length)".
- Tras la longitud del relleno se coloca el campo de 2 bytes "Siguiente cabecera (next header)" que especifica la siguiente cabecera.
- Por último, se añaden los 96 bits (8bytes) de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete, la cabecera IP no se incluye dentro de su proceso de cálculo.

Protocolo de Intercambio de Claves (IKE).

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras, que es la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo.
El protocolo IKE funciona en dos fases; La primera fase establece un ISAKMP SA (Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec.

- **Primera Fase:** Esta fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA.

La diferencia entre los dos modos es que el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo a pesar de ser más rápido, tiene sus desventajas, ya que el modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro y, por lo tanto, es susceptible a un ataque por usuario interpuesto.

- **Segunda Fase:** En esta fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques por usuario interpuesto. Esta segunda fase emplea el modo rápido.
Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

VPNs IPSEC

IPSec es un protocolo que a lo largo de los años, ha sido ampliamente utilizado para la creación de VPNs. Según las cifras de Forrester, el 62% de las empresas americanas utilizan IPSec para su acceso remoto y otro 20 por ciento asegura que lo están probando o poniendo en marcha. Como se digo anteriormente este protocolo fue introducido por la IETF como un conjunto de extensiones para IP, en este conjunto de estándares se incluyen las especificaciones para la distribución y encriptación de llaves simétricas:

IKE así como los servicios de autenticación sobre la capa IP. Cuando IPSec es usado para diseñar una VPN segura, este opera sobre la capa de red del modelo OSI esto lo hace independiente de las aplicaciones que se usen.

Las VPNs basadas sobre el protocolo IPSec trabajan estableciendo un túnel sobre el Internet fuera de los firewalls o Gateways de la organización. IPSec encapsula el paquete IP original en su propio paquete.

Una vez que el túnel se haya negociado mediante IKE, varias conexiones de diferente tipo pueden ser establecidas sobre este túnel, como por ejemplo: tráfico Web, email, transferencia de archivos, VoIP, etc.

Normalmente, para acceder a una VPN IPSec es necesario un software cliente que debe ser instalado en cada computador que desee acceder a la VPN, el cliente es configurado manualmente o automáticamente, depende de la solución específica para definir qué trafico debe ser enrutado sobre el túnel VPN.

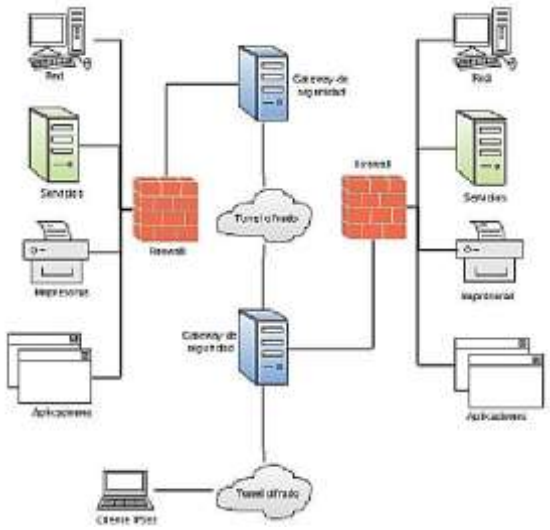


Figura No. 6.7: VPN sobre el protocolo IPSec.

Calidad de servicios sobre redes TCP/IP

Introducción

Las redes IP a mediados de los 90 eran redes de mejor esfuerzo y aún permanece con el mismo modelo, debido al rápido crecimiento, demandan recursos de calidad y hay algunas aplicaciones que son de mayor prioridad que las otras, tal es el casos de las aplicaciones de tiempo real, que requieren de tratamientos especiales. Internet no tiene la capacidad de diferenciar tráfico. Por lo tanto antes de que se puedan usar las aplicaciones de tiempo real, la infraestructura de Internet debe ser modificada. Algunas redes privadas han migrado de redes de mejor esfuerzo a redes de servicios diferenciados. IETF publicó un request for comment (RFC, petición de comentarios) referido a los servicios integrados. Estos documentos describen un protocolo de reservación de recursos RSVP. RSVP implementa una señalización antes que el flujo de datos sea enviado a la red, construyendo un canal virtual a lo largo del cual se reservan los recursos necesarios. Principalmente se reservan recursos de ancho de banda y latencia.

La ventaja de este mecanismo para los usuarios es que los recursos están estrictamente garantizados.

Aunque presenta la desventaja introduce una sobrecarga, que las redes amplias, como internet podrían volverse impracticables, debido a que existen muchos dispositivos de diferentes clases y fabricantes.

DiffServ es orientado a la no reservación, no establece canal virtual, en este modelo cada nodo interviniente adopta diferentes comportamientos de acuerdo a sus características. Esto soluciona el problema de overead, pero los recursos que necesitan los usuarios no están estrictamente asegurados.

Conceptos básicos de ip QoS

Las funciones IP QoS permiten a los proveedores de Internet (ISP) y proveedores de aplicaciones (ASP) ofrecer diferentes niveles de servicio de red a los clientes. Estas funciones permiten a las empresas e instituciones priorizar servicios para organizaciones internas o aplicaciones principales.

¿Por qué necesitamos QoS en las redes IP?

Las redes IP reparten paquetes con un tipo de servicio conocido como "best Effort" (BE), lo cual equivale a "lo más posible, lo antes posible". Los paquetes con este tipo de servicio tienen la misma expectativa de tratamiento a medida que transita la red. El router sólo mira el header, buscan en la tabla de ruteo y definen el próximo salto. Si llegase a ocurrir congestión, se retardan o descartan los paquetes. Esto hace muy escalable la red. Es suficiente para aplicaciones como mail, ftp y websurfing, pero no para otras aplicaciones que no toleran retardos variables o pérdida de datos, como es el caso de servicios de voz y video en tiempo real. Hay una convergencia de servicios no tradicionales: telefonía, radio, televisión, video conferencia, etc.; los cuales tienen otras exigencias. Una solución se podría pensar es agregar más ancho de banda, pero esto no es suficiente, ya que el tráfico es típicamente en ráfagas, produciendo congestiones temporales y retardos y pérdidas. Por lo tanto la clave está en dotar a Internet de una mayor "inteligencia", por medio de mecanismos para obtener QoS. El objetivo de la

calidad de servicio en una red es cuantificar el tratamiento que un paquete debe esperar a medida que circula por la red. El objetivo de una QoS diferenciada, es el dar a ciertos paquetes un mejor trato y a otros un peor trato.

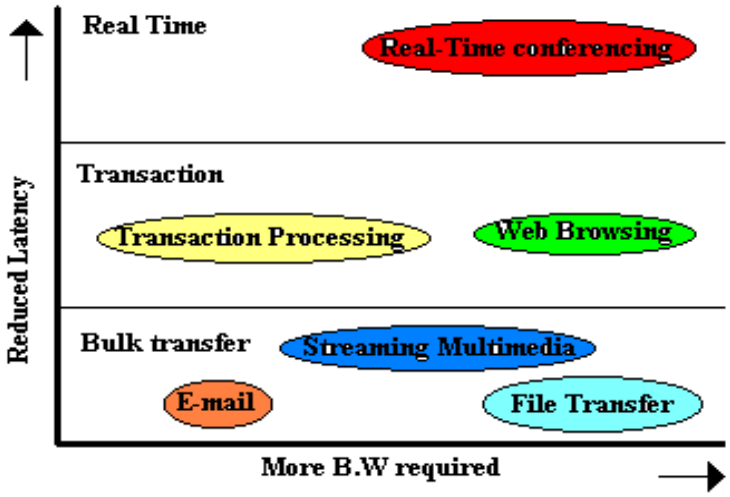


Figura No. 6.8: Paquete a medida que circula por la red.

Los proveedores de servicios en general publican un Acuerdo del Nivel de Servicio (SLA) para sus servicios, que contiene los niveles de calidad mensurables que un cliente espera del tráfico de la clase en particular que se encuentra manejando.

Las mayores aplicaciones iniciales que se esperan son:

- El distinguir la importancia del tráfico dentro de una nube de red
- El permitir una buena calidad de voz sobre redes IP. [3]

Parámetros de QoS y Objetivos

La QoS en redes IP puede ser caracterizada por un pequeño conjunto de parámetros medibles, relevantes para el tráfico de tiempo real.

- Disponibilidad de Servicio
- Retardo: Intervalo entre transmisión y recepción de un paquete entre dos puntos.

- Variación de retardo. Conocido como jitter referido a la variación del tiempo que tardan los distintos paquetes en una ruta.
- Throughput. Tasa en la cual los paquetes pueden ser transmitidos en una red, puede ser expresado en términos de valor máximo o promedio.
- Tasa de pérdida de paquetes.

Los objetivos de QoS en IP son proveer métodos para la optimización del ancho de banda y los tiempos de throughput, junto a la minimización en la pérdida de paquetes. Para ello se formulan diferentes estrategias:

- QoS en los Nodos de red. Una posibilidad es optimizar los nodos (routers, switches, etc.) por medio de técnicas de encolamiento en las interfaces.
- Señalización de QoS. Esto se puede lograr mediante el intercambio de información entre los nodos, de tal modo que se reserve ancho de banda para las aplicaciones individuales
- Manejo de Políticas QoS. Esto comprende un complejo procedimiento que involucra múltiples capas y requiere el monitoreo y control de todos los elementos de la red mediante reglas y políticas, desde una plataforma de gestión centralizada.
-

Calidad de servicios aplicados a VoIP

VoIP tiene características en su desempeño y por lo tanto necesita servicios de prioridad explicita. La deficiencia de las redes IP que afectan la voz son la pérdida de paquetes, la fluctuación de fase y retraso de manejo. Lo más común para resolver este problema es reproducir el paquete anterior, incrementando la atenuación en cada repetición. Por norma se acepta una pérdida de paquetes del 1%. La latencia el VoIP se caracteriza por el tiempo que tarde la voz en salir de la boca del transmisor hasta llegar al oído del receptor.

ECO

El eco siempre existirá en telefonía y es causado por reflexiones de la señal de voz. En general se pueden mencionar dos tipos de ecos. El primero denominado "eco directo" es deseable para quien habla y consiste en una pequeña realimentación de la voz propia de quien habla en su auricular otorgando una sensación de naturalidad al usuario. El segundo tipo "eco del auricular" es indeseable, puesto que la voz de la persona con quien se habla se detecta en forma doble. El eco siempre estará presente y se hará perceptible a contar de un retardo mayor que 25 [ms], que sobrepasando los 50 [ms], llega a considerarse molesto para la mayoría de los usuarios. Se puede aminorar el eco reduciendo la potencia de transmisión de las señales de voz.

Existen tres tipos de retraso:

- Retraso de señalización
- Propagación
- Manejo

RETARDO	TIPO	CAUSA
Procesamiento	fijo	Procedimiento de CODEC
Propagación	fijo	Propagación de la señal
Señalización	fijo	Ajustar el frame de voz a la red transporte (redes sincrónicas)
Encolamiento	variable	Causado por procedimientos de cola (paquetes que deben esperar para ser enviados en la línea)
De-Jitter	variable	Buffer para compensar los retardos variables

Tabla No. 6.1: Tipos de Retardo
Elaborado por: Freddy Robalino

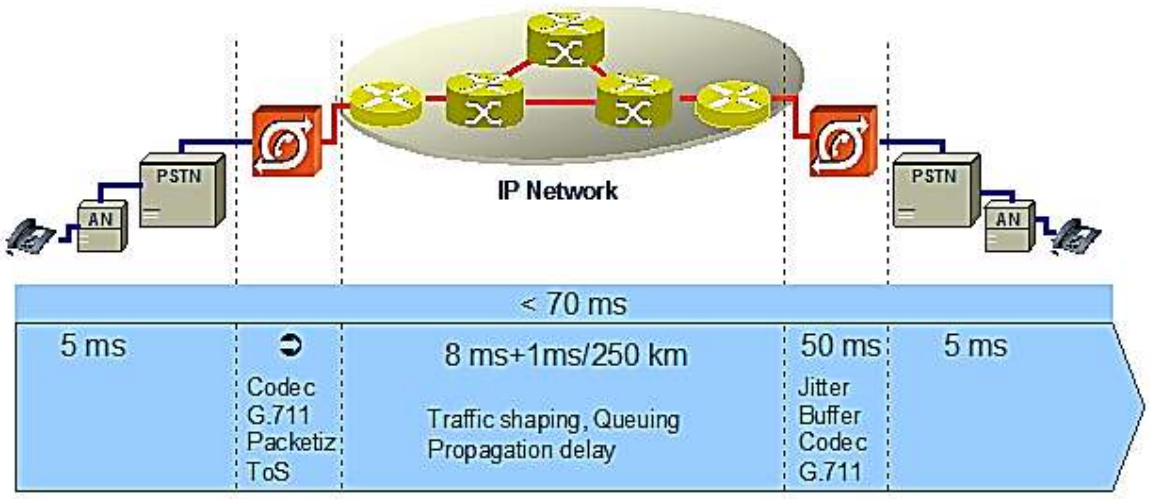


Figura No. 6.9: Retardo (ECO)
Elaborado por: Freddy Robalino

Ip VPN

Las IP VPN basada en MPLS brinda una de las soluciones de red como: rendimiento y mayor versatilidad; le ofrece auténtico alcance global, conectividad escalable, mayor seguridad, calidad de servicio garantizada, opciones de acceso múltiple y opciones de facturación flexibles.

VPN IP proporciona funciones de calidad de servicio (QoS), acceso a Internet gestionado y conectividad para usuarios remotos, que le permitirán garantizar unos niveles de rendimiento óptimos independientemente del lugar donde se encuentre. Este servicio se ofrece en distintas modalidades

VPN MPLS generación permite transportar diferentes tipos de tráfico IP, incluyendo tráfico de voz y datos, con calidad de servicio (QoS) y garantía.
Aquí se han estudiado los conceptos de QoS sobre redes IP, en la mismas se incluyen el uso integración de servicios como IPSec. A medida de que pasa el tiempo las aplicaciones demandan más recursos de red con calidad de servicios. IP tendrá que adoptar nuevos mecanismos de calidad de servicios para cumplir con los requerimientos de las aplicaciones futuras.

Metodología

El estudio contempla dos tipos de metodologías; una cuantitativa para el análisis estadístico de las variables e indicadores de seguridad en la transmisión de datos y otra cualitativa para el estudio de casos de modalidades asociativas, innovativas, y técnicas de calidad de servicio QoS[18] en la transmisión VoIP, además para el levantamiento de opiniones y percepciones respecto al diseño de la misma.

La cual permitirá en base a diseño de una red VPN con el protocolo IPSec brindar seguridad a la transmisión de datos VoIP en la F.I.S.E.I y la U.T.A.

Situación actual

Antecedentes

El presente trabajo fue planteado en Febrero del 2011 en donde la Universidad Técnica de Ambato y Facultad de Ingeniería en Sistemas, Electrónica e Industrial presenta los siguientes puntos relevantes.

Organización Actual de la Universidad Técnica de Ambato

La Universidad Técnica de Ambato se encuentra en la ciudad de Ambato capital de la provincia de Tungurahua, país Ecuador. Es la universidad más importante de la región central del país, cuenta con 10 facultades y 38 carreras en modalidad presencial y semipresencial.

Dispone de 16.000 estudiantes que se forman con un currículo por competencias y cuenta con una gran variedad de servicios como Internet, bibliotecas, servicio médico, odontológico, transporte, seguro estudiantil, comedor universitario, becas.

Para matricularse en una carrera universitaria de la Universidad Técnica de Ambato, debe inscribirse y rendir la Prueba de Aptitud Académica (PAA) de acuerdo al Calendario Académico.

Figura No. 6.10: Ubicación en el mapa de la U.T.A.

Figura No. 6.11: Campus Ingahurco

Figura No. 6.12: Campus Huachi

Misión

La misión de la Universidad Técnica de Ambato: satisfacer las demandas científico - tecnológicas de la sociedad ecuatoriana en interacción dinámica con sus actores, formar profesionales líderes con pensamiento crítico reflexivo, creativo con conciencia social que contribuya al desarrollo científico, técnico, cultural y axiológico del país; desarrollar la investigación científica y tecnológica como un aporte en la solución de los problemas; producir bienes y prestar servicios para contribuir al mejoramiento de la calidad de vida de los ecuatorianos e impulsar el desarrollo sustentable del país.

Visión

La Universidad Técnica de Ambato, por sus niveles de excelencia se constituirá en un centro de referencia académica científico y humanístico del país. Ser la institución que promueva la generación de proyectos y propuestas como soporte para el desarrollo provincial, regional nacional. En su entorno y tomando en

cuenta las manifestaciones del pensamiento del mismo creará conocimiento, formará profesionales competentes, realizará investigaciones científica y tecnológica, difundirá el arte y la cultura, promoverá el deporte y prestará servicios, proponiendo alternativas de solución a los problemas diversos sectores productivos y sociales. Estas acciones se realizarán en un ámbito de libertad, respeto a los derechos humanos e intelectuales, participación integrativa equidad de género y defensa del medio ambiente, con criterio de sustentabilidad y sostenibilidad.

Oferta Académica

Figura No. 6.13: Oferta Académica

La red Lan de la U.T.A

La "Universidad Técnica de Ambato" cuenta con una red privada que interconecta por medio de radio enlaces a los diferentes previos universitarios, que se encuentran ubicadas en diversos lugares de la ciudad, como se muestra en la siguiente figura.

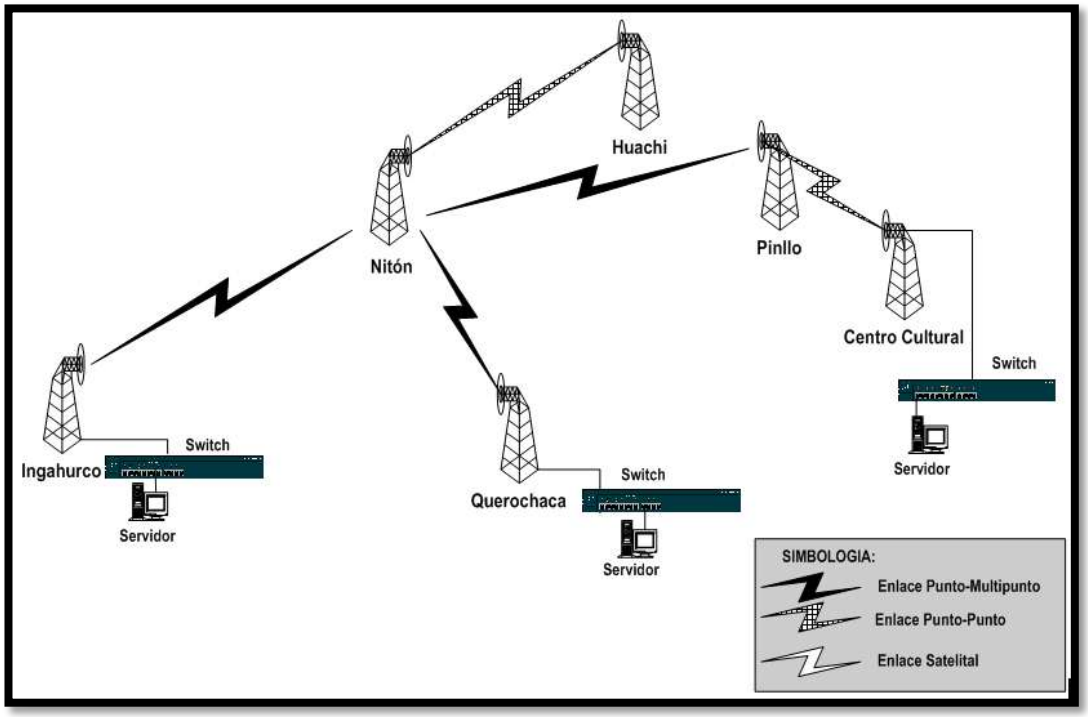


Figura No. 6.14: Red Privada de la UTA
Elaborado por: Freddy Robalino

La universidad cuenta con una estación base con un nodo de conexión de fibra óptica, con un ancho de banda de 28 MB que provee TELCONET y llega a los predios de Huachi, dispone de una red hibrida, que permite interconectar los diferentes predios universitarios.

La topología de red de propagación de señal, se realiza por medio de acceso inalámbrico punto – punto y punto – multipunto.

Radio enlaces

Tabla No. 6.2: Radio Enlaces de la Red de la UTA

Arquitectura	Descripción
Punto – Punto	Enlace previos de Huachi con la antena Nitón
Punto – Multipunto	Enlace antena Nitón, antena Pinllo
Punto - Multipunto	Antena Nitón con previos de Ingahurco
Punto - Multipunto	Antena Nitón con previos de Querochada
Punto - Punto	Antena Pinllo con Centro Cultural

Elaborado por: Freddy Robalino

La distribución de la señal se realiza a través de VLANS a las diferentes Facultades, por medio de un anillo de fibra óptica, a cada una se asigna 768 Kbps de ancho de banda.

Las facultades cuentan con cableado estructurado para sus redes LAN.

Servidores

El Departamento de Sistemas Informáticos y Redes de Comunicaciones, cuenta con los siguientes Servidores, que cumplen diferentes funciones, como son:

- **Cinco** servidores Linux, para la administración de redes de la universidad.
- **Dos** servidores 2003, Sistemas de información (UTAMATICO).

Adicionalmente, dentro de cada facultad existen servidores para la administración de sus redes locales y sus sistemas.

Estación Base

La arquitectura de estación base, provee el enlace con la infraestructura de fibra óptica y todo el tráfico dentro de esta infraestructura termina en suites o equipos de la oficina central.

- **Centro de Operaciones de la Red**.- Contiene un equipo de sistemas de administración de la red, se encarga de administrar y ampliar las redes.
- **Infraestructura de Fibra Óptica**.- Donde se realiza la conversión de la infraestructura de fibra a la infraestructura inalámbrica o cobre.
- **Cabecera.-** Soporta o facilita la transmisión de los diferentes servicios (datos, Internet), procesando la información y enviándola a todas las estaciones base.
- **Red de transporte**.- conecta la cabecera con otras redes

Redes de acceso al medio

En la Universidad, su red está constituida por varios segmentos:

- Red para laboratorios
- Red de facultades
- Red para servidores

Organización Actual de la Facultad de Ingeniería en Sistemas, Electrónica de Ambato.

Figura No. 6.15: Facultad de Ingeniería en Sistemas, Electrónica e Industrial
Elaborado por: Freddy Robalino

Topología de Red FISEI

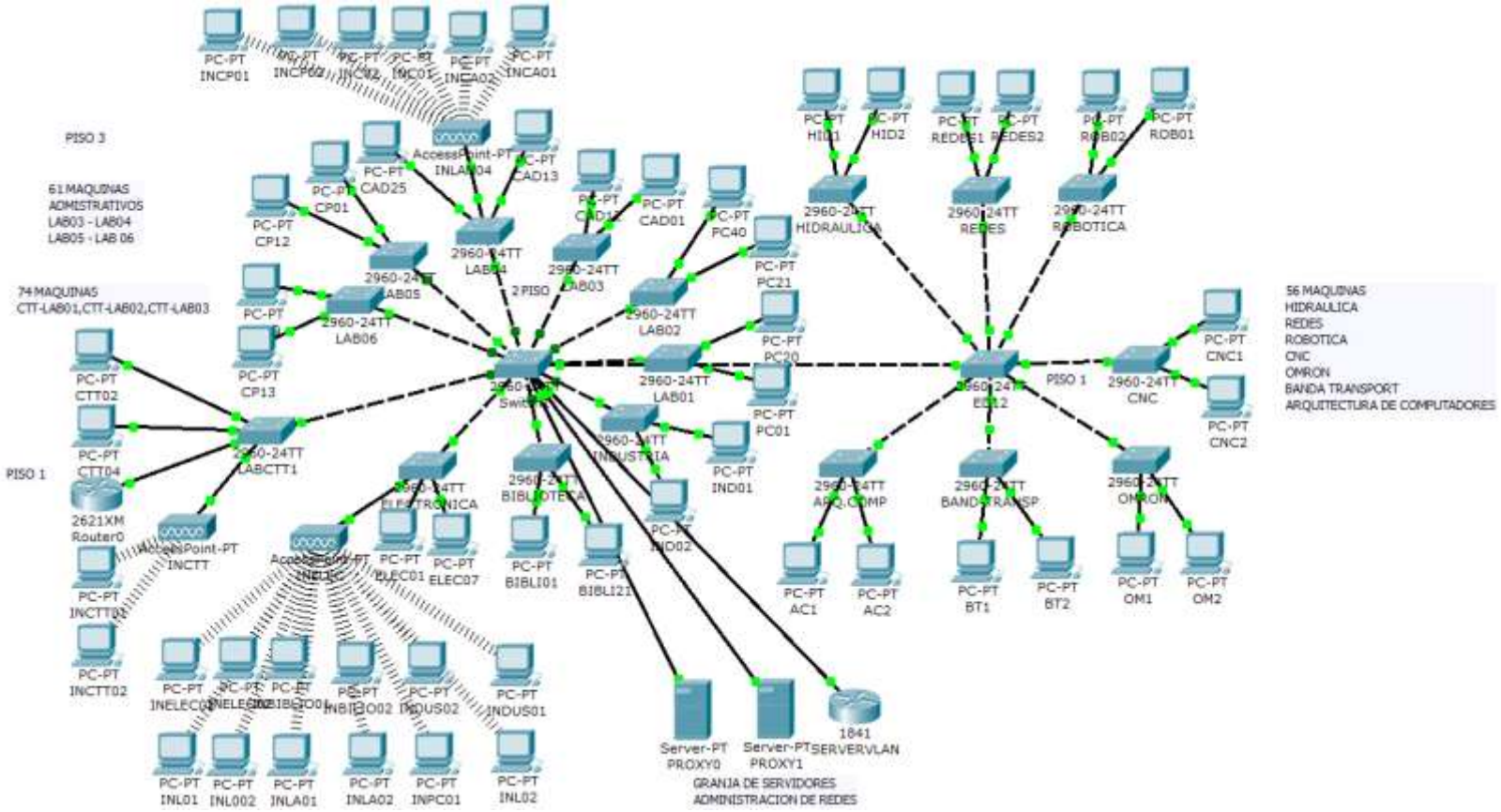


Figura No. 6.16: Topología de Red FISEI
Elaborado por: Freddy Robalino

Distribución Física de Equipos en la Red FISEI

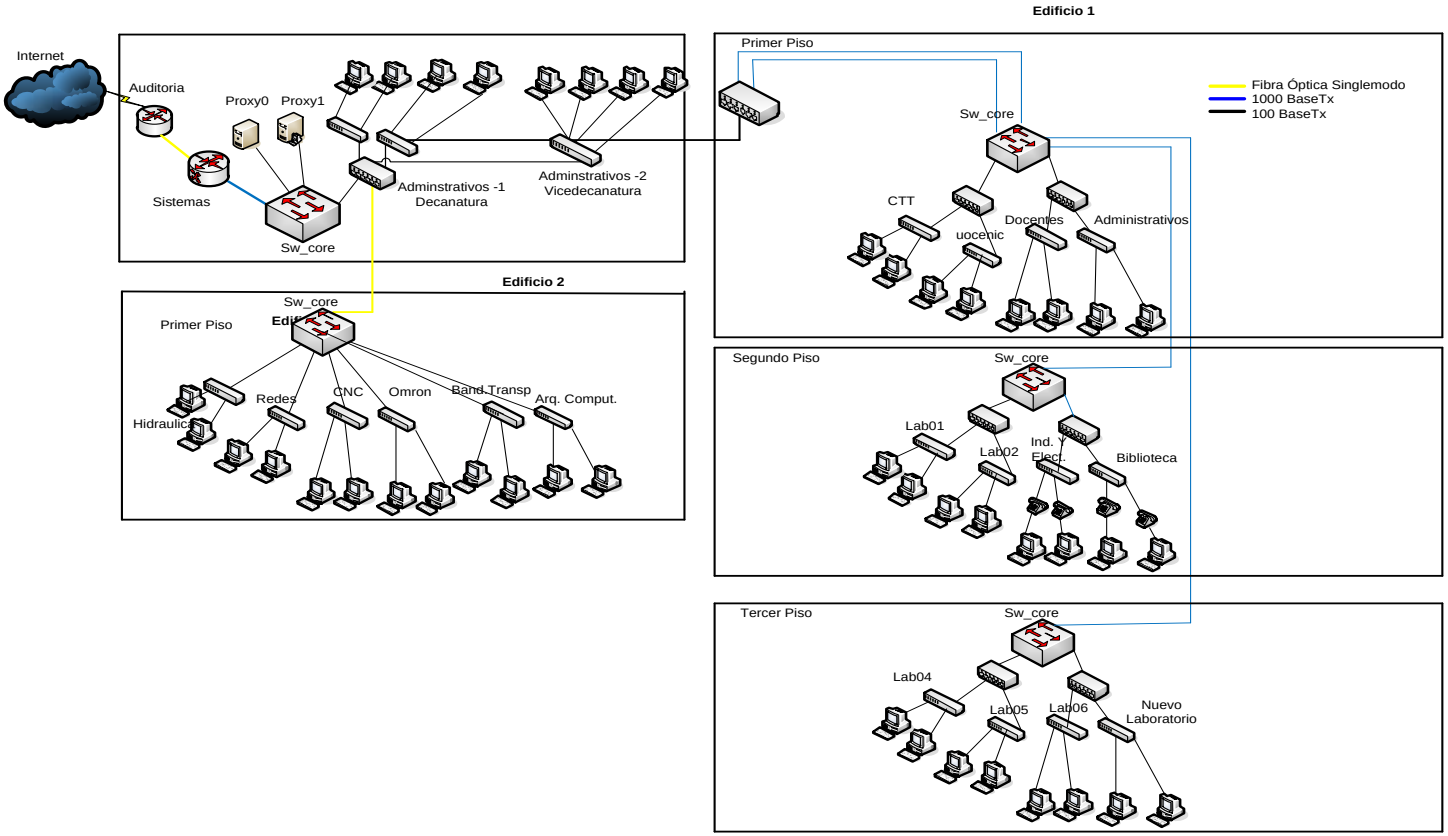


Figura No. 6.17: Distribución Física de Equipos
Elaborado por: Freddy Robalino

Laboratorios e instalaciones para desarrollo de investigación

Tabla No. 6.3: Instalaciónes de la Investigación

Laboratorio	Área	Carrera
1	Informática	**Básicos, Sistemas**
2	Informática	**Básicos, Sistemas**
3	Informática	**Básicos, Sistemas**
4	Informática	**Sistemas**
5	Informática	**Sistemas**
6	Informática	**Sistemas**
7	Redes	**Sistemas, Electrónica**
8	Industrial CAD-CAM	**Industrial**
9	Arquitectura computadoras	**Sistemas, Electrónica**
10	Robótica - Automatización	**Industrial, Electrónica**
11	Máquinas Eléctricas	**Industrial, Electrónica**
12	Electrónica Básica	**Electrónica**
13	Automatización OMRON	**Industrial, Electrónica**
14	Hidraulica-Neumatica	**Industrial**
15	CNC	**Industrial**
CTT		
1	Informática	**Estudiantes del FISEI y Servicios a la Colectividad**
2	Academia de Redes Cisco.	**Estudiantes del FISEI y Servicios a la Colectividad**
3	Informática-Redes	**Estudiantes del FISEI y Servicios a la Colectividad**

TALLERES		
1	Física Experimental	**Proyecto de Investigación FISEI**
2	**Electrónica e Industrial**	**Estudiantes FISEI tres carreras (Prácticas extracurriculares)**

Elaborado por: Freddy Robalino

15 laboratorios disponibles para la formación de los semestres básicos y las carreras de Ingeniería en Electrónica y Comunicaciones, Ingeniería Industrial en Procesos de Automatización e Ingeniería en Sistemas Computacionales e Informáticos.

3 Laboratorios del Centro de Transferencia de Tecnologías (CTT), al servicio también de los estudiantes en formación Extracurricular y de prestación de servicios, consultoría y capacitación a la colectividad

2 Talleres, de Física experimental con equipos de bajo costo (Proyecto de Investigación), y el 2do de formación extracurricular para prácticas de taller por parte de los estudiantes de las tres carreras.

Figura No. 6.18: Laboratorios CTT-FISEI-ACADEMIA CISCO
Tomado por: Freddy Robalino

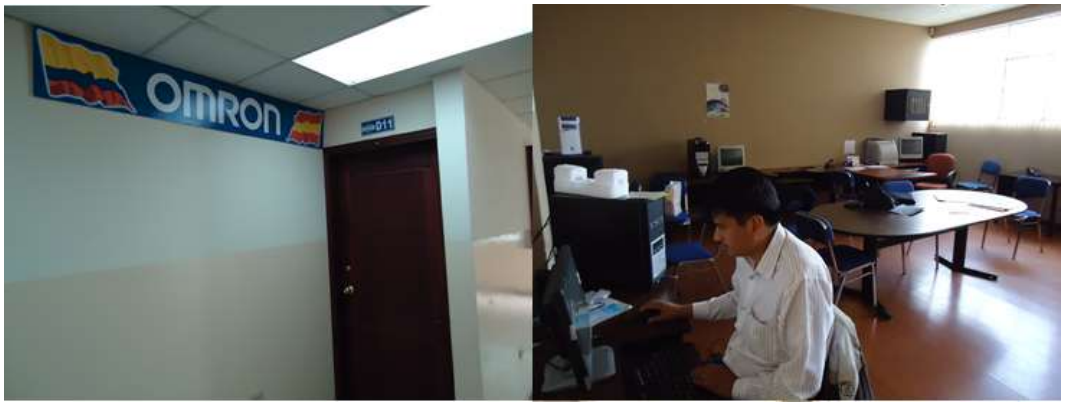


Figura No. 6.19: Laboratorios OMRON – UOCENIC
Tomado por: Freddy Robalino

Figura No. 6.20: Biblioteca y Laboratorio 2 de la FISEI.
Tomado por: Freddy Robalino

Equipos y sus Características

Tabla No. 6.4: Equipos, funciones y características.

Cantidad	Equipo / Configurado como:	Marca	Característica	Software	Ubicación
1	Servidor / Router	HP PROLIANT 3800	Processor Intel Xeon Processor 3.2 GHz standard Cache Memory 512KB level 2 cache and 2-MB level 3 cache Memory 1 GB) DDR SDRAM running at 266MHz with Advanced ECC Network Controller (2) NC7781 PCI-X Gigabit NIC Optical Drive 24x IDE CD-ROM (Universal Media Bay) Diskette Drive 1.44 MB Diskette Drive Form Factor Rack (2U), (3.5-inch)	S.O Via Console HP	Segundo Piso Administración de Redes Edificio 1
1	Servidor	HP Proliant ML350	1 or 2-way 1GHz processor 256 MBRAM Integrated single-channel Ultra2 SCSI drive controller Integrated NC3163 NIC (Fast Ethernet 10/100 Wake on LAN) SmartStart, Compaq Insight Manager/XE server management.	Windows Server 2003	Segundo Piso Administración de Redes Edificio 1
1	Servidor	Compac Proliant	Procesador(es) Pentium Pro 200Mhz/256K Memoria RAM 128 Mb Unidades 1 Disco SCSI 4.3GB Puertos 2 Puertos seriales, 1 Paralelo, Puerto de Red Rj45, BNC	Windows Server 2003 / Linux	Segundo Piso Administración de Redes Edificio 1
12	Switchs Acceso	3COM	Conmutador - 24 puertos Gestionado - apilable	S.O	Distribuidos

			Tipo incluido: Sobremesa - 1U Puertos: 24 x 10/100 + 2 x SFP + 2 x 10/100/1000, 24 x 10/100 + 2 x 10/100/1000 Tamaño de tabla de dirección MAC: 8K de entradas Unidades máximas en una pila: 4 Protocolo de direccionamiento: IGMPv2, IGMP Protocolo de gestión remota: SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, HTTP Método de autentificación: RADIUS Características: Control de flujo, conmutación Layer 2, auto-sensor por dispositivo, asignación dirección dinámica IP, negociación automática, soporte VLAN, snooping IGMP, activable, store and forward Cumplimiento de normas: IEEE 802.3u, IEEE 802.3i, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x Expansión / conectividad Interfaces: * 1 x consola - D-Sub de 9 espigas (DB-9) - gestión * 24 x 10Base-T/100Base-TX - RJ-45 * 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 * 2 x SFP (mini-GBIC) Dispositivo de alimentación: Fuente de alimentación – interna, Voltaje necesario: CA 120/230 V (50/60 Hz)	Via HTTP 3com	entre los: Edificio 1/ Edificio 2

Figura No. 6.21: Servidor 1 de Red –HP Proliant
Tomado por: Freddy Robalino

Figura No. 6.22: Servidor 2 y Servidor 3 (HP y Compac).
Tomado por: Freddy Robalino

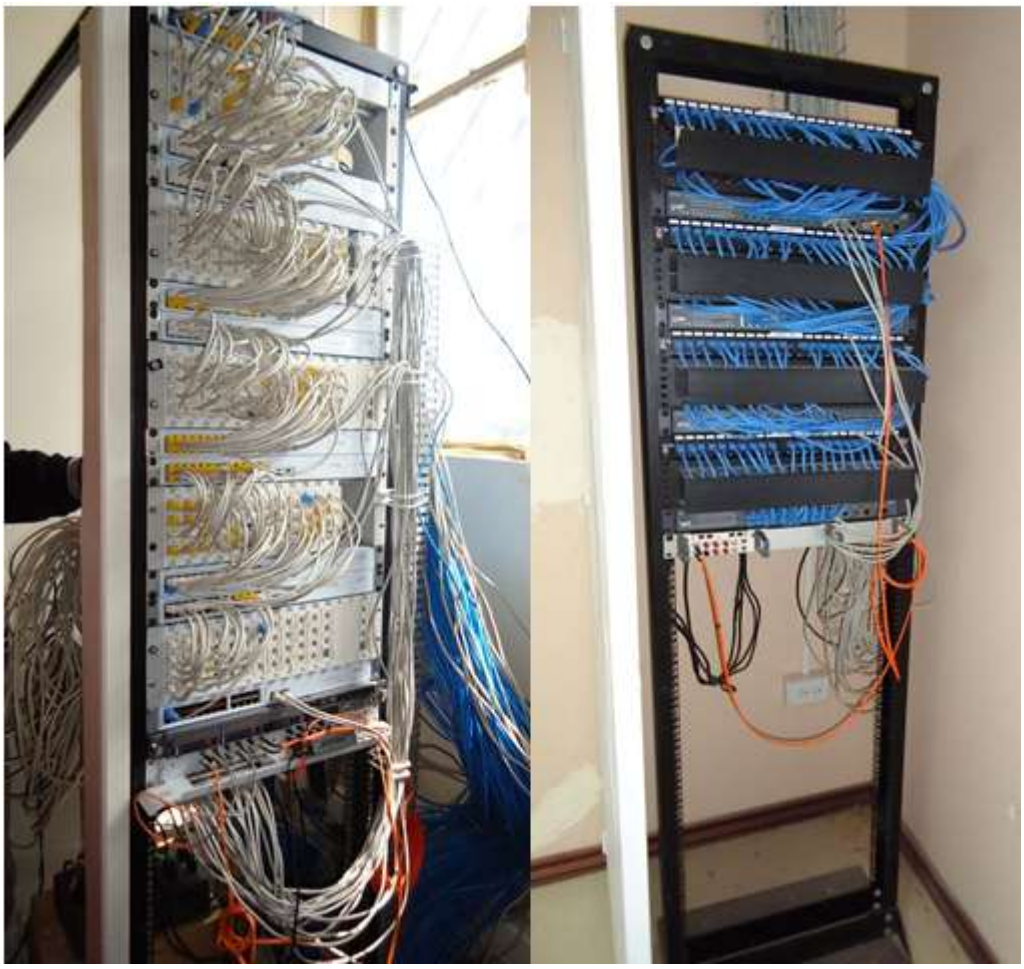


Figura No. 6.23: Racks para los Switchs 3COM.
Tomado por: Freddy Robalino

Equipos existentes reutilizables

Debido a que el diseño se basa en la seguridad de transmisión de los datos a nivel de la capa de distribución, todos los equipos de la capa de núcleo (Servidores) y acceso (Switchs) se pueden reutilizar; solo se necesita añadir a la topología de red los dos equipos de Security Appliance (ASA 5510) en la capa donde se hace el ruteo de paquetes (Capa de distribución).

Equipos por adquirir

Luego de una entrevista con el administrador de la red, supo manifestar que no se ha considerado la compra de equipos de seguridad, solo equipos de terminales (computadores).
Pero manifiesta que en caso de implantarlos, existe una partida dentro de la facultad proveniente de los programas de maestrías que haciende aproximadamente a 25000 Usd, para la compra de estos equipos.

Diseño de la Red

Las redes privadas virtuales ofrecen una alternativa segura para la transmisión de datos e interconexión de redes a través de la red e internet, utilizando lo que se conoce como un túnel VPN. Este permite que la información viaje de manera segura por un medio de comunicación, y de forma encriptado, ilegible para todos excepto para el destinatario.

Esta propiedad abre una alternativa para instituciones y empresas de todo tipo que requieren transportar su información de manera segura, mientras permiten a usuarios geográficamente separados, acceder de forma segura a la red LAN de la institución o empresa. Cualquier tipo de aplicación que se tenga en una Intranet (LAN) podrá acceder por medio de esta alternativa. Por ejemplo, acceder remotamente a los recursos de la red, a un servidor de bases de datos, compartir documentos, impresoras y, en el presente caso, brindar el servicio de VoIP, en si transmitir datos.

Para el desarrollo de la propuesta se considera un ambiente empresarial típico conformado por una estación matriz y una estación sucursal, en nuestro caso el Campus Ingahurco y Campus Huachi respectivamente, enfocando el Campus Huachi donde se encuentra la red de la FISEI.

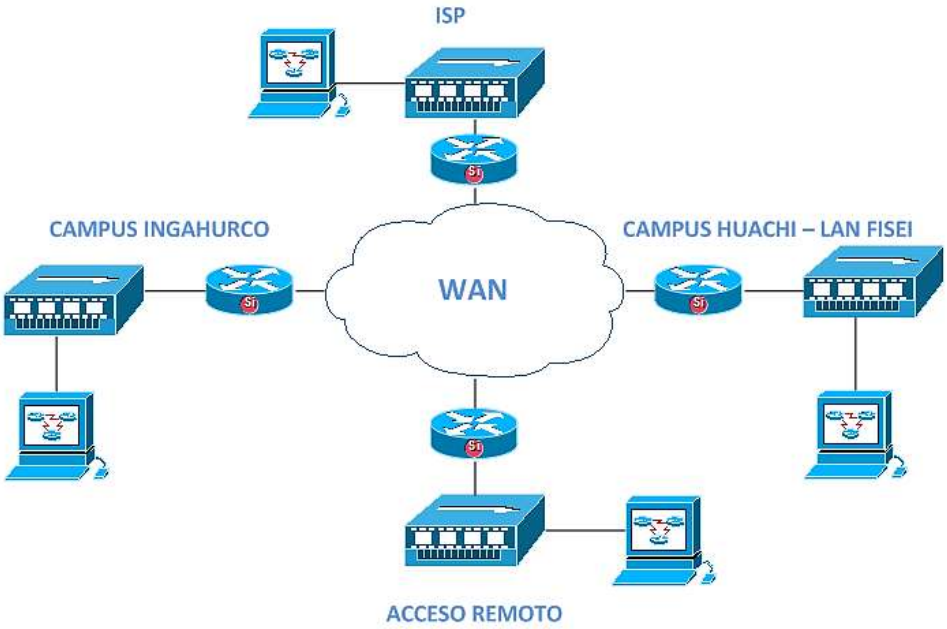


Figura No. 6.24: Esquema de la Topología de Red Propuesta.
Elaborado por: Freddy Robalino

El propósito del diseño es definir reglas técnicas, para efectuar un túnel VPN con IPSec a través de una nube WAN, formada por varios routers interconectados.

La red VPN a diseñar brindara seguridad, además de la integridad, confidencialidad y autenticación, para las comunicaciones VoIP entre los campus y especialmente la red de la F.I.S.E.I.

Descripción de la topología de red propuesta

Podemos empezar explicando que una VPN puede ser construida en diferentes topologías como: Internet VPN, ***Intranet VPN*** y Extranet VPN. En el caso de una Intranet VPN se crea un canal de comunicaciones privado sobre las redes abiertas de Internet.

Este tipo de VPN cumple con las siguientes funciones:

- Brindar conectividad segura a departamentos, dependencias u oficinas separadas, a través de Internet.

- Brindar conectividad segura a usuarios a través de un ISP(WAN).

En una Intranet VPN se debe habilitar un canal de comunicaciones privado sobre la infraestructura de la red LAN de la Institución, entidad bancaria, campus universitario, etc. De esta manera se utiliza una Intranet VPN para brindar acceso seguro a los datos e información privilegiada además de sitios privados dentro de la entidad.

A su vez en una Extranet VPN se maneja un canal de comunicaciones privado entre dos o más sitios separados. Esto implica transmisión de datos seguros a través de un enlace WAN, como Internet. Se utilizara una Extranet VPN para comunicar la red de la institución con redes de clientes o entidades afines.

Requisitos

En el presente proyecto se desea crear una conexión entre los campus, y dentro de la LAN de la F.I.S.E.I por tal razón los datos a transmitir serán de la misma entidad. Este es un ambiente de trabajo asociado a una Intranet VPN que cumple con relacionar dependencias u oficinas de la misma institución.

Entre las empresas que podrían tener una infraestructura como la que aquí se cita, se destacan: cadenas de supermercados, de farmacias, universidades, etc. La cual nuestra facultad y la universidad cuenta. Adicional a esto todas aquellas entidades que tienen oficinas y empleados o trabajadores que requieran trabajar remotamente.

Descripción de la red propuesta en el Campus Ingahurco

La Universidad Técnica de Ambato y la Facultad de Ingeniería en Sistemas como una Institución educativa, donde la cantidad de estudiantes va en incremento día con día, estos potenciales usuarios de la red y de los servicios que proporciona la misma debe contar con un esquema como el propuesto, esquema denominado de 3 capas.

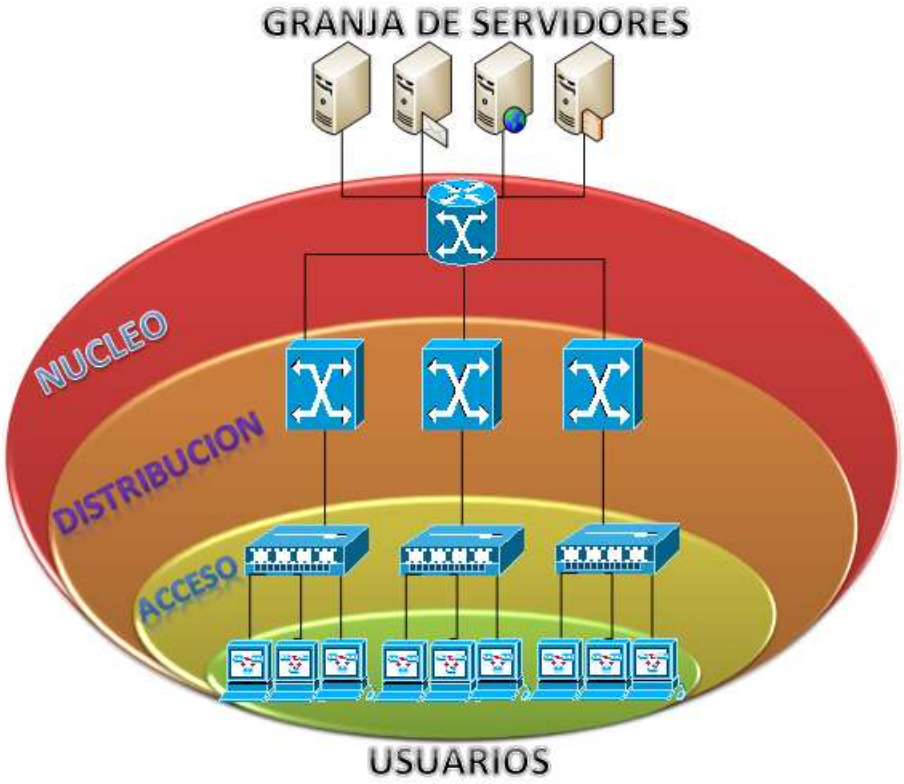


Figura No. 6.25: Esquema Diagrama de Red Campus Ingahurco
Elaborado por: Freddy Robalino

En extracto, la capa de acceso proporciona a los usuarios de grupos de trabajo acceso a la red. La capa de distribución ofrece conectividad a los usuarios basada en políticas, mientras que la capa núcleo llamada también backbone proporciona transporte óptimo entre sitios.

Los switchs de la capa de acceso operan en la Capa 2 del modelo OSI y ofrecen servicios como el de asociación de VLAN. El principal propósito de un switch de capa de acceso es permitir a los usuarios finales el acceso a la red. Un switch de capa de acceso debe proporcionar esta funcionalidad con bajo costo y una alta densidad de puerto acorde al número de usuarios que se tengan proyectados. En los switchs de acceso es donde se conectaran los PCs que funcionaran con el softphone que permitirá hacer y recibir llamadas por Internet con VoIP o a su vez teléfonos IP.

El switch de la capa de distribución es un punto en el cual se encuentra limitado el dominio de broadcast[19]. Se pueden aplicar políticas de seguridad a través de listas

de control de acceso que se encargan de filtrar paquetes. *La capa de distribución aislará los problemas de red dentro de los grupos de trabajo* en los cuales se producen. La capa de distribución también evita que estos problemas afecten la capa núcleo. La capa de distribución combina el tráfico VLAN y es un punto focal para las políticas de red de la institución sobre transporte de datos y el flujo de tráfico. Por estas razones, los switchs de la capa de distribución operan tanto en la Capa 2 como en la Capa 3 del modelo OSI. Los switchs en esta capa se conocen como switchs multicapa.

El campus Ingahurco cuenta con departamentos Financiero, Administrativo, Docente, Estudiantil. Para ello cuenta con VLANs y políticas que van de acuerdo a cada área de trabajo, dando así una mejor administración y servicio a los usuarios de la red.

La capa núcleo es un backbone de conmutación de alta velocidad. Esta capa no debería realizar ninguna manipulación de paquetes. La manipulación de paquetes, como por ejemplo el filtrado mediante listas de acceso, hace que la conmutación de paquetes se vuelva lenta. Una infraestructura central con rutas alternadas redundantes ofrece estabilidad a la red en caso de que se produzca una única falla en un dispositivo. Esto garantiza a los usuarios el acceso permanente a los servidores que dispone la red.

En el campus Ingahurco funciona actualmente una red LAN que permite a todos sus usuarios una conexión a Internet. Se cuenta con un número de 70 potenciales usuarios que mantendrían comunicación activa, y que a su vez de 18 a 20 requieren acceso telefónico.
Los usuarios en la red LAN del campus requieren mantener los siguientes servicios o aplicaciones:

- Correo Electrónico.
- Descarga de archivos.
- Navegación Web.

- Acceso a bases de datos.

Los servidores deben ir lo más próximo a la capa núcleo. Esto permite a los usuarios el rápido acceso a los servicios mencionados anteriormente. Un servidor de VoIP se debe conectar en esta capa.

Descripción de la red propuesta en el Campus Huachi – FISEI

Esta red cuenta con menor número de usuarios y menor requerimiento de recursos de red, por lo que utiliza un esquema reducido de 2 capas, acceso y distribución. En este caso la capa de distribución realiza las funciones de la capa núcleo.

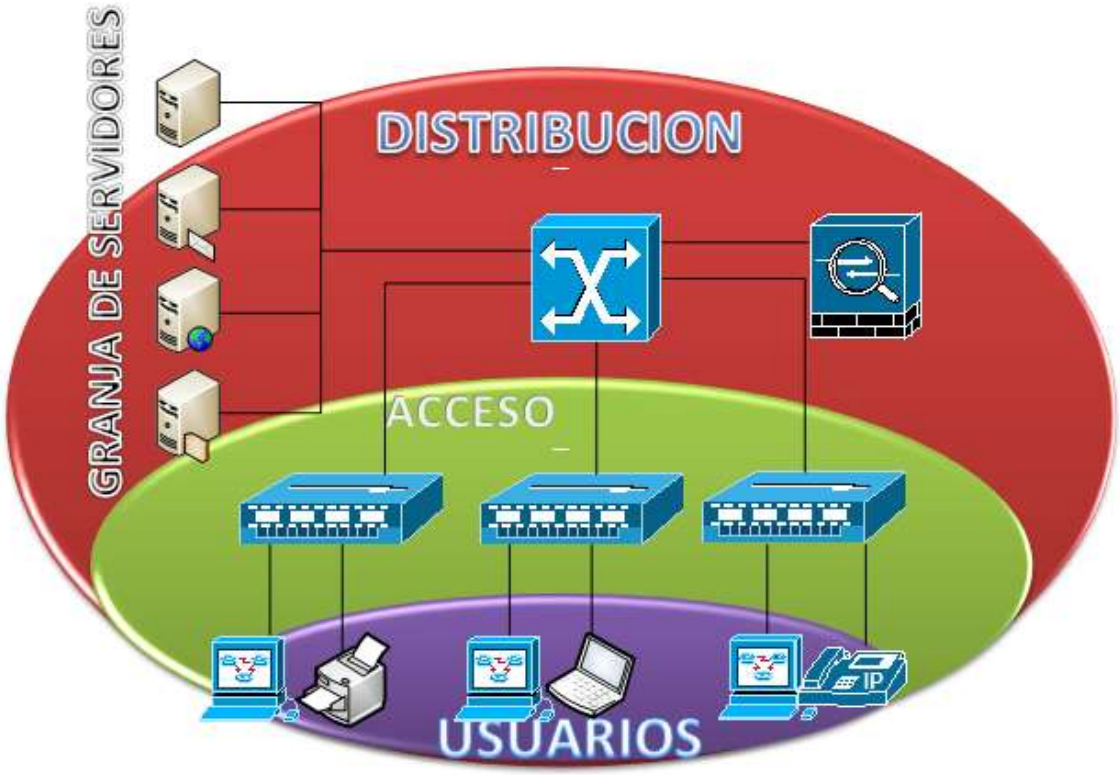


Figura No. 6.26: Esquema Diagrama de Red Campus Ingahurco

Los usuarios en esta dependencia mantienen los mismos servicios que los usuarios en el Campus Ingahurco, a saber:

- Correo Electrónico.
- Descarga de archivos.

- Navegación Web.
- Acceso bases de datos.

Escenario VPN

De acuerdo con los requisitos planteados se proponen las siguientes soluciones VPN.

Intranet VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la institución o empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la institución o empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes LAN e Inalámbricas.

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MAC Address, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna.

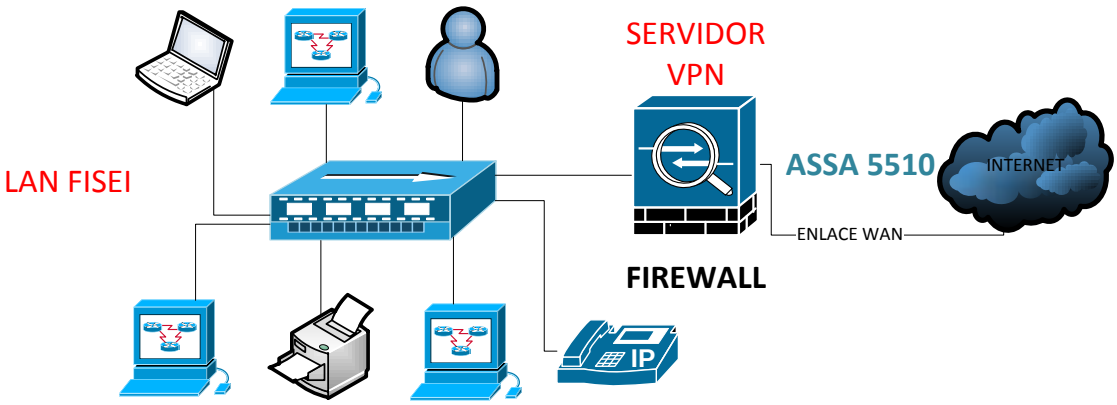


Figura No. 6.27: Esquema Topología de Red VPN sobre la LAN
Elaborado por: Freddy Robalino

Intranet VPN Sitio A Sitio

Con este esquema se puede acceder a los recursos de una red LAN desde otra. En este caso se permitirá el acceso dentro de la misma, de cada uno de las dependencias de todo el campus indistintamente de donde se origine la llamada y desde los dos campus.

La siguiente topología muestra un ejemplo de una conexión de tipo sitio a sitio. Como se pude ver, es una conexión independiente de la distancia entre cada una de las redes.

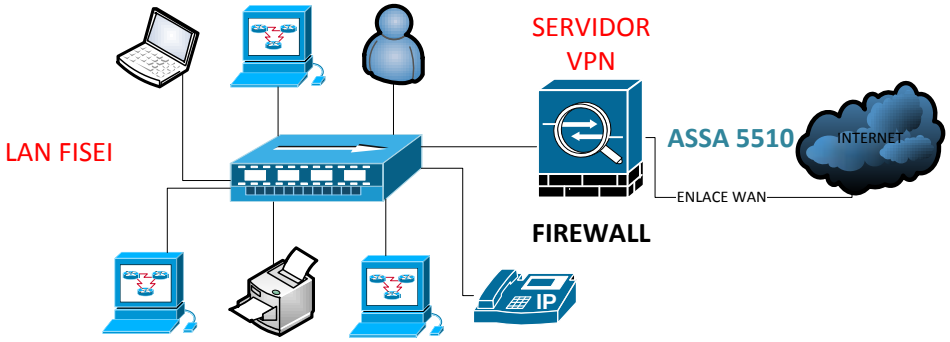


Figura No. 6.28: Esquema Topología de Red VPN de LAN a LAN.
Elaborado por: Freddy Robalino

Para topología se plantea el uso de 2 equipos de borde, que soportarán el túnel VPN. Un equipo ubicado en el campus Ingahurco y el otro en Huachi, en ellos se configuraran los comandos necesarios para poder procesar y transmitir información encriptada, previo a la autenticación y acreditación del par respectivo. De esta manera, la red telefónica tendrá una administración centralizada ubicada en la oficina matriz en Quito porque contiene el mayor número de extensiones.

Las aplicaciones y servicios de otros empleados que no hagan uso del túnel VPN no se verán afectadas de ninguna manera en el momento en que el túnel empiece a operar. De esta manera se permite independencia al nuevo servicio de VoIP y del normal desempeño de los otros servicios y aplicaciones en curso. Para cumplir esta finalidad se limita a los usuarios el acceso al túnel mediante listas de acceso permitiendo el uso únicamente a los usuarios que transmiten paquetes VoIP.

Diseño de la VPN

Para el diseño de la VPN se deben cumplir con ciertos requisitos, los cuales se describen a continuación.

Asignación de direcciones

El direccionamiento de las redes LAN internas se realiza de acuerdo a la norma RFC 1918. Ésta indica el rango de direcciones privadas.

Clase	Desde	Hasta	Cantidad de bits para Red	Cantidad de bits para Host
A	10.0.0.0	10.255.255.255	8	24
B	172.16.0.0	172.31.255.255	16	16
C	192.168.0.0	192.168.255.255	24	8

Tabla No. 6.5: Direcciones Privadas.
Elaborado por: Freddy Robalino

Hay que tener claro que al utilizar direcciones IP privadas no es posible conectase directamente a Internet por lo tal razón se necesita la traducción de direcciones de red (NAT) a una dirección pública enrutable.

El rápido crecimiento de la Internet ha sorprendido a la mayoría de los observadores. Una de las razones por las que Internet ha crecido tan rápidamente es debido a la flexibilidad del diseño original. Sin el desarrollo de nuevas tecnologías de asignación de direcciones IP, el rápido crecimiento de Internet habría agotado la cantidad actual de direcciones IP. Para poder compensar esta falta de direcciones IP, se buscaron diferentes soluciones. Una solución ampliamente implementada, es la Traducción de direcciones de red.

La Traducción de direcciones NAT es un mecanismo de conservación de direcciones IP registradas en las grandes redes y simplificar las tareas de administración de direccionamiento IP. Mientas se enruta un paquete a través de un dispositivo de red, por lo general un firewall o router fronterizo, la dirección IP fuente se traduce de una dirección de red interna privada a una dirección IP pública enrutable. Esto permite que se transporte el paquete a través de redes externas públicas como la Internet. La dirección pública de la respuesta se traduce de nuevo a la dirección interna privada para su entrega dentro de la red interna. Una variación de NAT, conocida como Traducción de direcciones de puerto (PAT), permite la traducción de muchas direcciones privadas internas con una sola dirección pública externa como se puede ver en la siguiente figura.

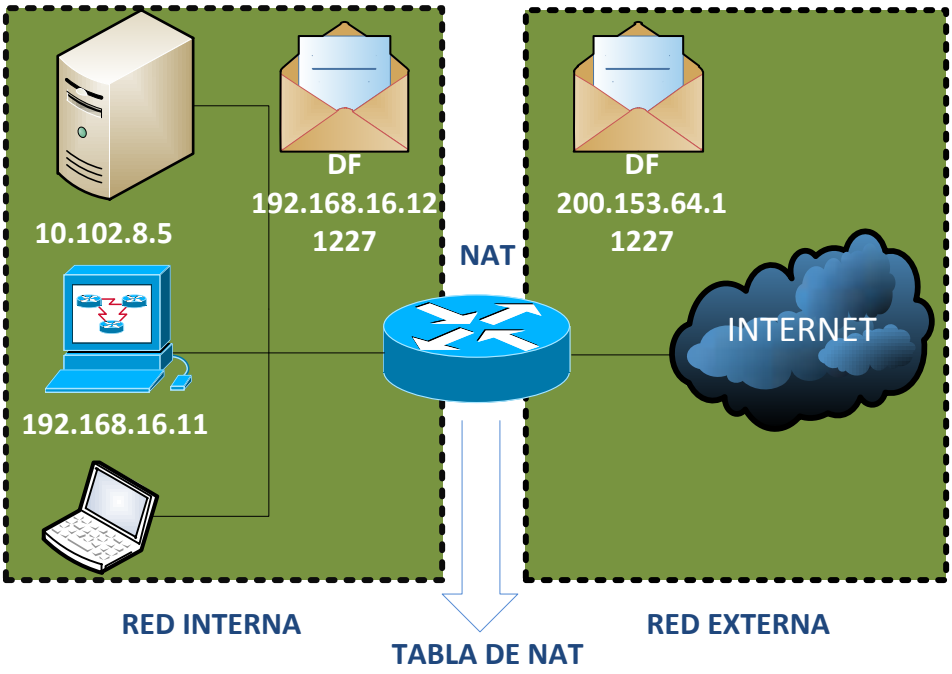


Figura No. 6.29: Tabla de NAT
Elaborado por: Freddy Robalino

DIRECCIÓN IP PUERTO INTERNO	DIRECCIÓN IP PUERTO EXTERNO
10.102.8.5 : 1227	**200.153.64.1 : 1227**
192.168.16.11: 1250	**200.153.64.1 : 1227**

Tabla No. 6.6: Esquema de direccionamiento IP red LAN
Elaborado por: Freddy Robalino

Así mismo se describe la dirección que utilizan las direcciones IP privadas para comunicarse a Internet, en el caso en que no se encuentren conectadas a la red VPN.

RED	RANGO DE DIRECCIONES	TRADUCCIÓN DE DIRECCIONES	PUERTA DE ENLACE	MASCARA DE RED
Ingahurco	10.102.8.1	-	10.102.8.4	255.255.255.0
Huachi	10.102.8.5 Subredes:	200.153.64.1 / 27	10.102.8.17	255.255.255.0 Subredes:

	192.168.0.0 – 192.168.255.255			192.168.0.0 – 192.168.255.255

Tabla No. 6.7: Asignación de Direcciones.
Elaborado por: Freddy Robalino

Un usuario remoto estará sometido a un proceso de asignación dinámica de direcciones llevado a cabo por el equipo encargado de realizar la autenticación y control de acceso a la red, que en este caso se localizará en el campus Ingahurco, y tendrá una dirección en el rango de direcciones de la misma.

Protocolos Seguros para VPN

Existen varios protocolos para el establecimiento de túneles VPN, como PPTP, L2F, L2TP, que funcionan en capa 2 del modelo de referencia OSI, y que además permiten establecer conexiones remotas. Pero a diferencia del resto IPSec además permite mantener sesiones remotas y que, a diferencia de los mencionados anteriormente, funciona en capa 3; pero lo más importante de IPSec es que permite autenticar los paquetes mientras viajan por la red, a diferencia de los protocolos mencionados anteriormente que permiten autenticar los paquetes únicamente en los extremos del túnel.

Por lo tanto el protocolo que se utilizará para el túnel VPN es IPSec que permite brindar seguridad a nivel de capa 3, lo que significa que cada paquete IP se encapsula con una cabecera IPSec.

IPSec provee un mecanismo para brindar seguridad en la transmisión de datos, a través de redes IP, brindando confidencialidad, integridad y autenticación de datos para comunicaciones sobre redes no protegidas tal como es el Internet. IPSec para ambientes VPN se caracteriza por:

- Confidencialidad de datos: El dispositivo que envía los datos puede encriptar los paquetes antes de transmitir éstos a través de la red.

- Integridad de los datos: El dispositivo que recibe los datos puede autenticar el otro equipo (peer) y paquetes IPSec recibidos para asegurarse que los datos no han sido alterados durante la transmisión.
- Autenticación del origen de los datos: El dispositivo IPSec receptor puede autenticar la fuente de los paquetes IPSec que son enviados de forma independiente de la integridad de los datos; es decir, que se verifica el origen de los datos independientemente de la cantidad de errores.
- Anti-Replay: El dispositivo IPSec receptor puede detectar y rechazar paquetes repetidos ayudando a prevenir Vishing, Spoofing, y ataques errados.

Por otra parte, los dispositivos de seguridad que se vayan a utilizar deberán soportar, además de IPSec, otros protocolos como:

- ESP (Encapsulation Security Payload) Los dispositivos IPSec utilizan ESP para encapsular paquetes IP.
- IKE (Internet key Exchange) IKE es un protocolo híbrido que provee servicios útiles para IPSec como:
  - Autenticación de los pares IPSec
  - Negociación IKE y asociaciones de seguridad IPSec
  - Establecimiento de llaves por algoritmos de encripción usados por IPSec

De igual manera se requiere de algoritmos criptográfico como:

- DES (Data Encryption Standard)
  DES es usado para encriptar y desencriptar paquetes de datos.
  DES es usado tanto por IPSec como por IKE.
- 3DES (Triple Data Encryption Standard)
  3DES es una variación de DES y tiene tres llaves separadas.
  3DES triplica la fuerza de encripción de DES; es decir, tiene una llave de 168 bits.
  3DES es usado para encriptar y desencriptar el tráfico de datos.

- AES (Advanced Encryption Standard)

  AES provee mayor seguridad que DES y es más eficiente que 3DES.

  The National Institute of Standars for Technology (NIST) recientemente adoptó el nuevo algoritmo de encripción AES para reemplazar a DES en dispositivos criptográfico.
- DH (Deffie - Hellman)

  DH es un protocolo criptográfico de llaves públicas. Este permite dos partes para establecer una llave secreta compartida sobre un canal de comunicaciones inseguro.
- MD5 (Message Digest)

  MD5 es un algoritmo hash usado para autenticar paquetes de datos. Un hash es una forma de algoritmo de encripción que toma un mensaje de entrada de una longitud arbitraria y produce una variación de la longitud en el mensaje de salida.
- IKE y ESP usan MD5 para la autenticación.
- SHA (Secure Hash Algorithm) SHA es un algoritmo hash usado para autenticar paquetes de datos. - IKE y ESP usan SHA-1 para la autenticación.

Al analizar estos algoritmos se ha decidido usar el algoritmo de encripción AES, porque permite el uso de llaves de diferente tamaño, además porque ha demostrado ser mucho más eficiente que su predecesor DES. AES ha sido adoptado por organizaciones y entidades a nivel internacional y desde su nacimiento no se conoce ningún ataque que haya podido burlar la seguridad que ofrece este algoritmo.

Selección de los Equipos

Para crear una conexión VPN se puede utilizar cualquiera de los routers indicados a continuación ya que una buena parte de equipos de la red de la uta son cisco y los que no en 2011 serán reemplazados por las marca CISCO, y además de que estos proveen mayores y mejores servicios de seguridad para los datos.

- Cisco 806, Cisco 826, Cisco 827, y Cisco 828 Routers.
- Cisco 1700 Series Routers.
- Cisco 2600 Series Routers.
- Cisco 3620 Router.
- Cisco 3640 Routes.
- Cisco 3660 Router.
- Cisco 7100 Series VPN Routers.
- Cisco 7200 Router.
- Cisco CVPN3002-8E-BUN-K9
- Cisco 7500 Series Routers.
- Cisco 5510 Series ASA. (Firewall Cisco ASA 5510)

Al momento de elegir un equipo se debe tomar en cuenta las aplicaciones previas que tiene la institución o empresa, por ejemplo: El acceso a Internet y la compartición de recursos con el fin de mantener la Intranet funcional, como venía operando previo a la implementación del túnel VPN; es decir, que la implementación del túnel sea transparente a los usuarios dentro de la LAN que no requieran de acceso a través del túnel VPN.

Para propósitos de prueba de la conexión VPN se utilizan dos equipos Cisco ASA (Adaptive Security Appliance) Serie 5510.

Figura No. 6.30: Equipos Cisco ASA 5510

Los equipos ASA son firewalls con varias funciones y características, de las cuáles se consideran importantes para la presente propuesta:

- Dispositivo para medianas y grandes empresas que brindan seguridad y aplicaciones VPN.

- Interfaces Giga ethernet10 / 100 / 1000 Mbps
- Soporta VPN sitio a sitio (LAN to LAN)
- Soporta VPN de Acceso Remoto
- Soporta WebVPN
- Virtual Firewalls
- Protocolo de interconexión de datos: Ethernet, Fast Ethernet
- Capacidad del cortafuegos : 300 Mbps
- Tasa de conexiones : 6000 sesiones por segundo
- Capacidad de la VPN : 170 Mbps
- Capacidad Peers VPN IPSec : 250
- Peers VPN SSL : 2
- Sesiones concurrentes : 50000
- Interfaces virtuales (VLAN) : 50
- Cantidad de túneles VPN 50 túneles
- Características Protección firewall, asistencia técnica VPN, soporte VLAN
- Algoritmo de cifrado DES, Triple DES, AES

Pasos para establecer la sesión VPN utilizando IPSec

Para establecer una comunicación, debe previamente establecerse un túnel VPN, que en el presente proyecto es un requisito de seguridad importante. En una secuencia de 5 pasos, resumidos de acuerdo a los procedimientos que se van ejecutando, IPSec levanta el túnel VPN que servirá de enlace entre los campus, o a su vez entre oficinas, entidades y un Usuario Remoto.

Especificar el tráfico de interés (Enrutamiento Dinámico)

El tráfico se denomina de interés o (enrutamiento dinámico) cuando el dispositivo VPN reconoce que el tráfico que se quiere enviar necesita ser protegido. En este caso se define como tráfico interesante a los paquetes de voz (VoIP).

El método para esto es por medio de listas de acceso (Access List), ya que de esta manera se habilitarán los puertos tanto TCP como UDP que sean necesarios para la transmisión de voz y, de ser necesario, algún otro puerto que necesite de encripción. A pesar de que el protocolo ICMP no necesita ser encriptado, se requiere para probar conectividad, por lo que se habilitaría como tráfico interesante, temporalmente.

Los puertos que no se vayan a utilizar deben ser bloqueados de tal manera que el tráfico que pase a través del túnel sea exclusivamente el que requiere ser encriptado y autenticado.
Las políticas de seguridad institucionales son las que deben definir que tráfico necesita ser protegido y cuál tráfico debe ser enviado en forma plana; es decir, sin la necesidad de encriptar.

Los usuarios de la Intranet pueden comunicarse con los usuarios de la Intranet asociada a través del túnel VPN, o pueden, simplemente, navegar por la Internet para lo cual no es necesario acceder al túnel VPN. El control de acceso al túnel se realiza en el equipo de borde y es aquí donde se identifica el tráfico de interés y se conduce por el túnel VPN, mientras que el tráfico no interesante se desplaza abiertamente por la red pública.

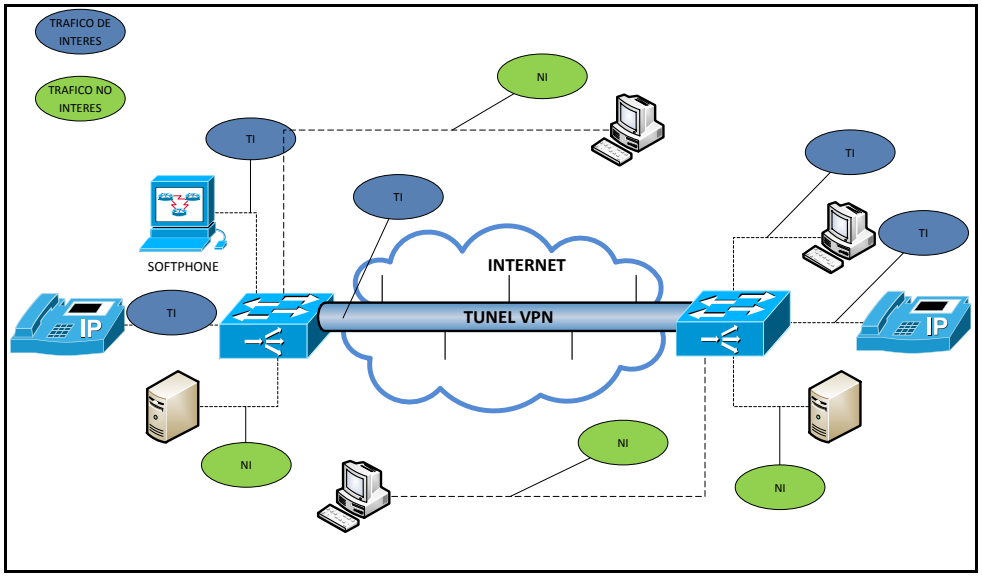


Figura No. 6.31: Trafico de Interés – Enrutamiento Dinámico
Elaborado por: Freddy Robalino

Establecimiento de la conexión

En esta fase se establece la conexión entre los extremos del túnel. Para el establecimiento de la conexión se necesita una configuración básica de servicios de seguridad que son negociados y acordados previamente entre los pares (peers) de la VPN. Estos servicios de seguridad protegen todas las subsecuentes comunicaciones entre los pares.

Para este diseño se propone utilizar el protocolo IKE para el establecimiento de la conexión, para ello se dice que IKE actúa en dos fases. El propósito básico de IKE fase 1 es negociar políticas de configuración IKE (algoritmo de encripción, de autenticación, tiempo de vida del túnel), autenticación de los pares y configurar un canal seguro entre los mismos.

Establecimiento de las Políticas de Seguridad

Las políticas de seguridad se establecen para definir el grado de seguridad que se debe brindar a los datos a transmitir. Empieza por discriminar entre los datos que necesitan seguridad y los que no; por ejemplo, al momento de definir el tráfico interesante, que es cuando se define el tipo de paquetes que requieren seguridad, y una vez definido el tráfico interesante se define que parámetros son necesarios para cumplir los requisitos de seguridad impuestos por la empresa.

Las políticas de seguridad se establecen en la segunda fase de IKE. El propósito en ésta fase de IKE es negociar los parámetros de seguridad de IPSec que son usados para asegurar el túnel VPN.

IKE fase 2 cumple con las siguientes funciones:

- Negociar parámetros de seguridad IPSec.
- Establecer Asociación de seguridad IPSec

Periódicamente renegocia asociaciones de seguridad para IPSec de esta manera cumple con aspectos de seguridad como integridad confidencialidad, etc. Opcionalmente mantiene un intercambio DH.

Transmisión de datos

Una vez negociadas las políticas de seguridad; es decir, luego de que la segunda fase de IKE ha sido completada, se establece una sesión IPSec para lo cual se establecen asociaciones de seguridad IPSec. El tráfico se intercambia entre los host de la redes a través de un túnel seguro. El tráfico interesante es encriptado y desencriptado de acuerdo con los servicios de seguridad especificados en el IPSec.

Finalización de la conexión

Una vez hecha la comunicación, la sesión del túnel puede darse por finalizada por las siguientes razones:

- Cuando el tiempo de la conexión o sea el Lifetime configurado en los parámetros llega a su fin.
- Si excede el valor configurado del contador de paquetes.
- Cuando es removido o eliminado el IPSec SA.

Estimación de Ancho de Banda

El ancho de banda requerido para una aplicación VoIP depende mucho del códec que se utilice. Existen algunas normas y estándares de compresión, caracterizados por el Mean Opinión Score (MOS) que es un valor con escala del 1 al 5, como se muestra en el siguiente Figura.

Este parámetro se utiliza para resaltar la calidad presente en un determinado códec, pero pese a que los diferentes códecs requieren de diferentes velocidades de transmisión, la calidad en términos de MOS no se ve considerablemente disminuida entre el de menor y mayor MOS. Por ejemplo, en el caso de G.711 el MOS indicado es de 4.1, mientras que para el caso de G.729 el MOS es de 3.92.

La principal diferencia está en las capacidades de transmisión requeridas en los diferentes códecs; en el caso de G.711 se requiere de 64 Kbps, en tanto que para G.729 se requiere una capacidad de 8 Kbps, Para hacer un mejor uso del ancho de banda se considera el estándar G.729 como norma para este proyecto, que por una parte ofrece un MOS bastante aceptable y por otra disminuye considerablemente los requerimientos de ancho de banda para una aplicación VoIP.

Por tal razón y aunque debido a los resultados obtenidos anteriormente en la simulación el mejor desempeño es el códec G.711 se propone escoger el G.729 por su BIT RATE y MOS.

NOMBRE	ESTÁNDAR	DESCRIPCIÓN	BIT RATE (KB/S)	FRAME SIZE (MS)	MOS (MEAN OPINION SCORE)
G.711	ITU-T	Pulse code modulation (PCM), Ley A y Ley μ	**64**	Muestreada	**4.1**
G.722	ITU-T	7 kHz audio-coding within 64 Kbit/s	**64**	Muestreada	**-**
G.723	ITU-T	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones	**24/40**	Muestreada	**-**
G.723.1	ITU-T	Dual rate speech code for multimedia Communications transmitting at 5.3 and 6.3 Kbit/s	**5.6/6.3**	30	**3.8-3.9**
G.726	ITU-T	40, 32, 24, 16 Kbit/s adaptive differential pulse code modulation (ADPCM)	**16/24/32/40**	Muestreada	**3.85**
G.728	ITU-T	Coding of speech at 16 Kbit/s using low-delay code excited linear prediction	**16**	2.5	**3.61**
G.729	ITU-T	Coding of speech at 8 Kbit/s using conjugate-structure Algebraic code excited linear-prediction (CS-ACELP)	**8**	10	**3.92**
GSM	ETSI	Regular Pulse Excitation Long Term Predictor (RPE-LTP)	**13**	22.5	-

Tabla No. 6.8: Códecs que soporta Asterisk
Elaborado por: Freddy Robalino

A continuación se procede a calcular el ancho de banda requerido para un canal de voz. En esta parte se tiene que considerar los protocolos que intervienen en la transmisión de un paquete de voz. A saber:

- Cabecera UDP y RTP, que en conjunto suman 20 bytes (8 bytes UDP y 12 bytes RTP). Cabe recalcar que SIP, protocolo utilizado para señalización de voz, se ubica dentro de RTP.
- Cabecera IP, que tiene un tamaño de 20 bytes.
- Cabecera IPSec., de acuerdo al protocolo que se utilice, ESP o AH.
- Protocolo de capa 2, que puede ser PPP.

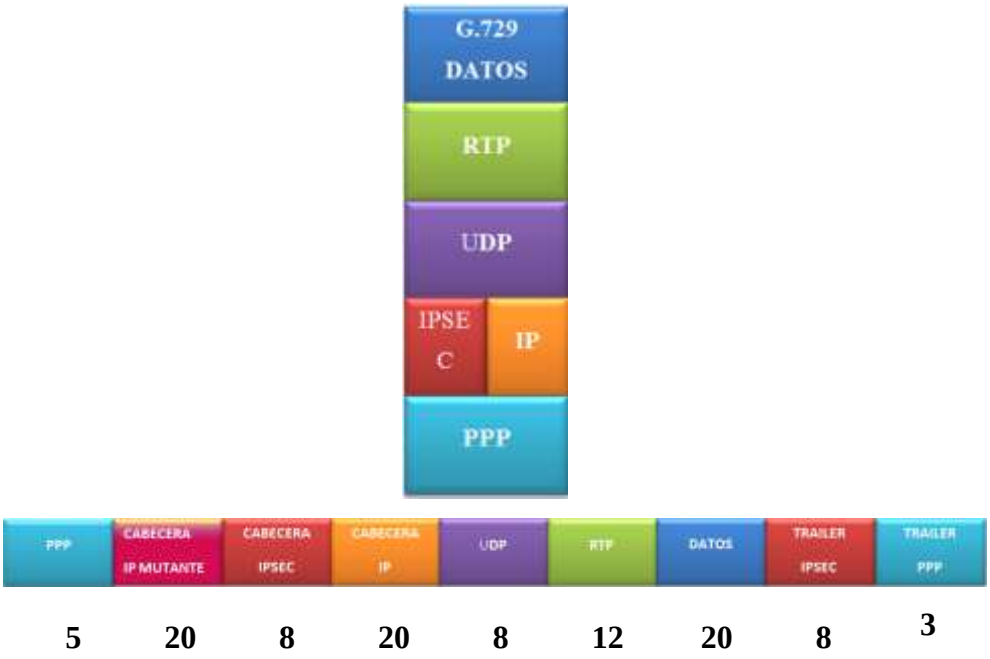


Figura No. 6.32: Proceso de Encapsulamiento VoIP y Trama de datos.
Elaborado por: Freddy Robalino

Considerando que un códec G.729 transmite paquetes de 20 bytes a una velocidad de 8 Kbps se calcula que transmite 50 paquetes por segundo (PPS), se tiene la siguiente Ecuación

DATOS:
Velocidad= 8Kbps
Cantidad de paquetes=20 bytes

$$PPS = \frac{8\ Kbps}{8bits\ x\ 20\ bytes}$$

$PPS = 50$ Paquetes por segundo

Para esto se ha considerado las cabeceras y trailers de los protocolos que intervienen en el proceso de encapsulamiento:

Cantidad de Paquetes	20 bytes
Cabecera y Trailers	84 bytes
Total	**104 bytes**

Tabla No. 6.9: Cantidad de Paquetes.
Elaborado por: Freddy Robalino

AB (kbps) = 104 bytes x 8bits x 50 PPS

AB (kbps) = 41.600 bps

AB (kbps) = 41,600 Kbps

Entones este es el ancho de banda que debe tener un canal VoIP considerando los protocolos de seguridad y de encapsulamiento ya mencionados. Para cumplir con una demanda de 15.85 Erlangs, se requiere de 19 canales de 41.6 Kbps, que significa un ancho de banda de 790.4 Kbps.

Este cálculo se puede aproximar con la ayuda de una calculadora de ancho de banda para aplicaciones VoIP en el sitio http://blog.asteriskguide.com/bandcalc/bandcalc.php , en la que se puede aproximar el cálculo dependiendo del protocolo utilizado. Se puede así mismo estimar un ancho de banda de acuerdo al número de llamadas simultáneas.

A continuación se muestra el cálculo utilizando una conexión VPN, con el protocolo IPsec como herramienta de seguridad, además se elige PPP como protocolo de capa 2.

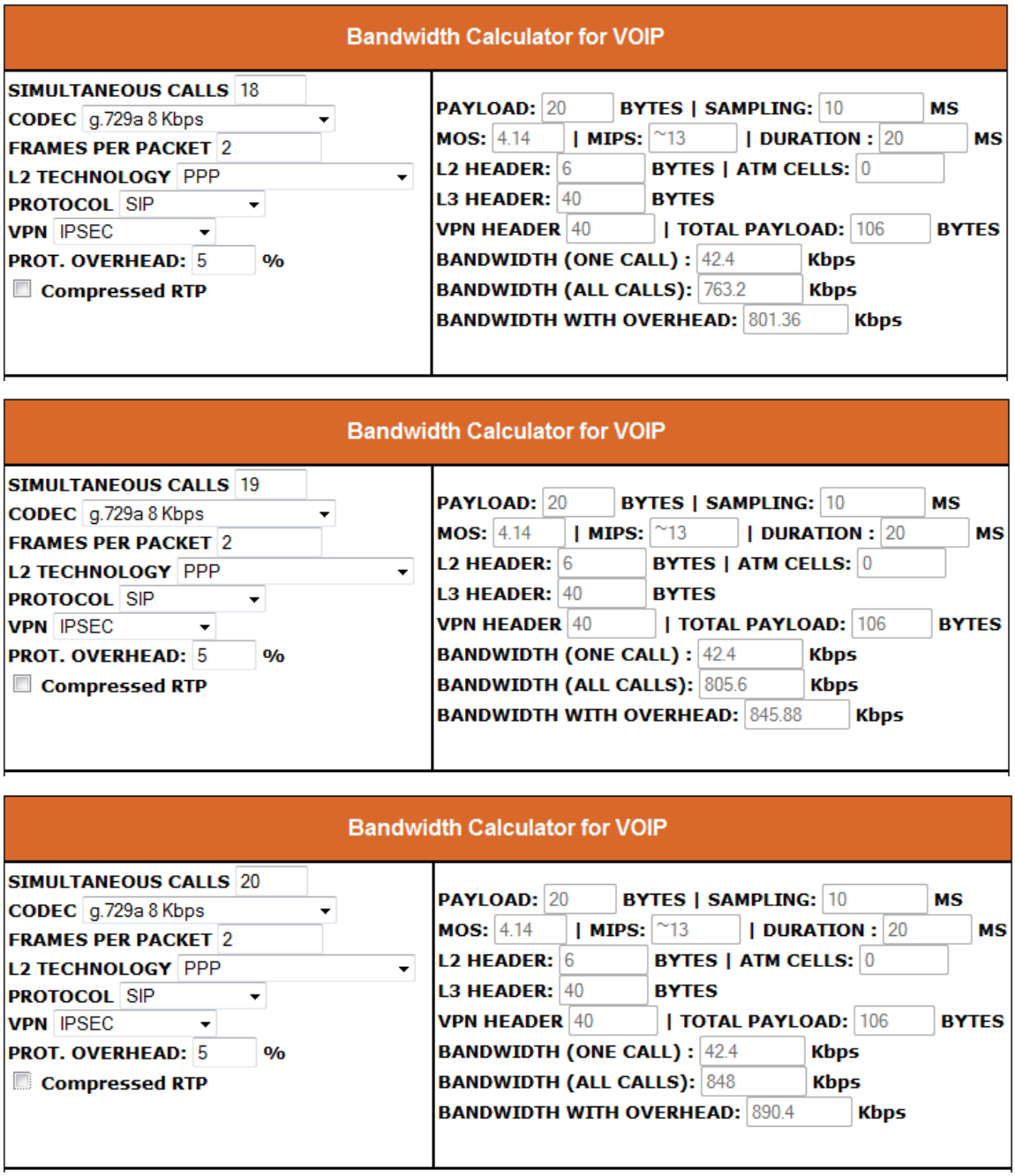


Figura No. 6.33: Calculo de ancho de banda VoIP.
Elaborado por: Freddy Robalino

Según el cálculo y la estimación de ancho de banda se deberá contar con un ancho de banda de al menos 1024 Kbps, mientras se tenga un excedente de ancho de banda se tendrá un menor porcentaje de pérdidas.

Estudio de factibilidad para implementación de una red telefónica administrada bajo Linux.

Podemos empezar entendiendo la diferencia entre IPtel e IP Telephony es la cobertura que puede limitar uno u otro servicio. En el caso del servicio de VoIP, la cobertura de una llamada no se limita a un espacio físico específico; es decir, que la llamada puede acceder a cualquier punto sobre la red de Internet, con una cobertura a nivel de WAN. Telefonía IP da un servicio de tipo LAN que conlleva un manejo administrativo tanto de recursos como de usuarios más detallado y centralizado.

Con la aplicación de Telefonía IP sobre VPNs es posible conectar a usuarios remotos a una red local, permitiendo de esta manera mantener una comunicación entre campus sin perder el control sobre los terminales remotamente conectados.

Existen herramientas de software de código abierto que soportan aplicaciones Telefonía IP como Asterisk Now que brinda cobertura telefónica a nivel de central telefónica, PBX. Asterisk ha sido diseñada para trabajar en diferentes escenarios en cuanto a cobertura se refiere.

En un ambiente WAN, Asterisk administra a un grupo de extensiones ubicadas en localidades diferentes, por ello se utiliza como herramienta para manejar una central PBX que satisfaga las necesidades.

En siguiente topología se observa que el servidor Asterisk se puede ubicar en el campus Huachi en la red de la FISEI. Con sus respectivas extensiones los usuarios se podrán registrar en un servidor Asterisk pudiendo así llamar o recibir llamadas entre usuarios de la toda la red.

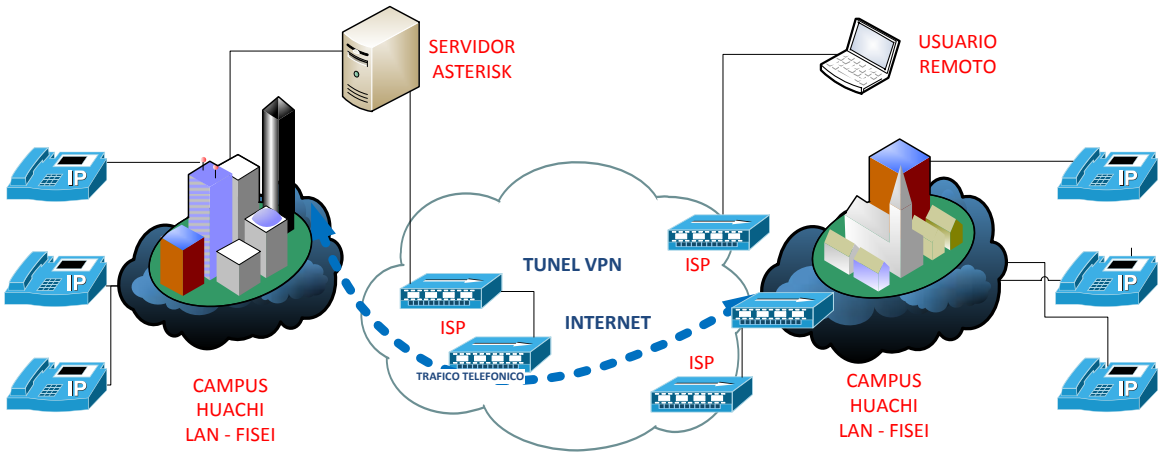


Figura No. 6.34: Posible Esquema Telefónico de la Red
Elaborado por: Freddy Robalino

ORIGEN	DESTINO
Usuario Remoto	Ingahurco
Usuario Remoto	Huachi
Ingahurco	Ingahurco
Ingahurco	Huachi
Ingahurco	Usuario remoto
Huachi	Ingahurco
Huachi	Huachi
Huachi	Usuario remoto

Tabla No. 6.10: Tabla Origen – Destino de llamadas.
Elaborado por: Freddy Robalino

Asterisk

Asterisk es un programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios. Esta plataforma soporta principalmente sistemas operativos basados en UNIX17, como Linux, FreeBSD, Solaris entre otros.

Su licencia permite distribuir libremente Asterisk en forma de código fuente. La GPL no está referida al hardware o software con el que Asterisk se comunica; por ejemplo, si se utiliza un softphone SIP, teléfono que soporta protocolo SIP, como cliente de Asterisk, este no requiere que el software también sea distribuido bajo los términos de la GPL.

Asterisk está creada para ofrecer una interface entre cualquier parte del software o hardware telefónico y/o los servicios telefónicos que esta ofrece y de manera transparente. Tradicionalmente, los productos telefónicos son diseñados para resolver una necesidad específica dentro de la red; sin embargo, muchas de las aplicaciones y servicios telefónicos más usados necesitan implementar gran cantidad de tecnología que no siempre está incluida en el precio de la PBX.

Asterisk toma ventaja de esta sinergia, para crear un único ambiente que puede amoldarse y encajar adecuadamente en cualquier aplicación, ofreciendo todos los servicios que el usuario estime conveniente.

Arquitectura Asterisk

Asterisk actúa como intermediario, conectando tecnologías telefónicas con aplicaciones y servicios telefónicos de forma transparente creando de esta manera un ambiente que permite unificar varias tecnologías y poder desplegar una telefonía mixta.

El núcleo de Asterisk contiene varias engines (máquinas) las cuales participan en la operación del software. Las Interfaces de Programas de Aplicación API específicas, como se muestran en la siguiente figura, son definidas alrededor del núcleo del sistema. El núcleo se ocupa de la interconexión interna de la plataforma, separándose de los protocolos específicos, códec, interfaces de hardware y de las aplicaciones telefónicas. Esto le permitirá a Asterisk usar cualquier hardware conveniente y tecnología disponible ahora o en el futuro para

realizar sus funciones esenciales, conectando hardware y aplicaciones en la red de la universidad.

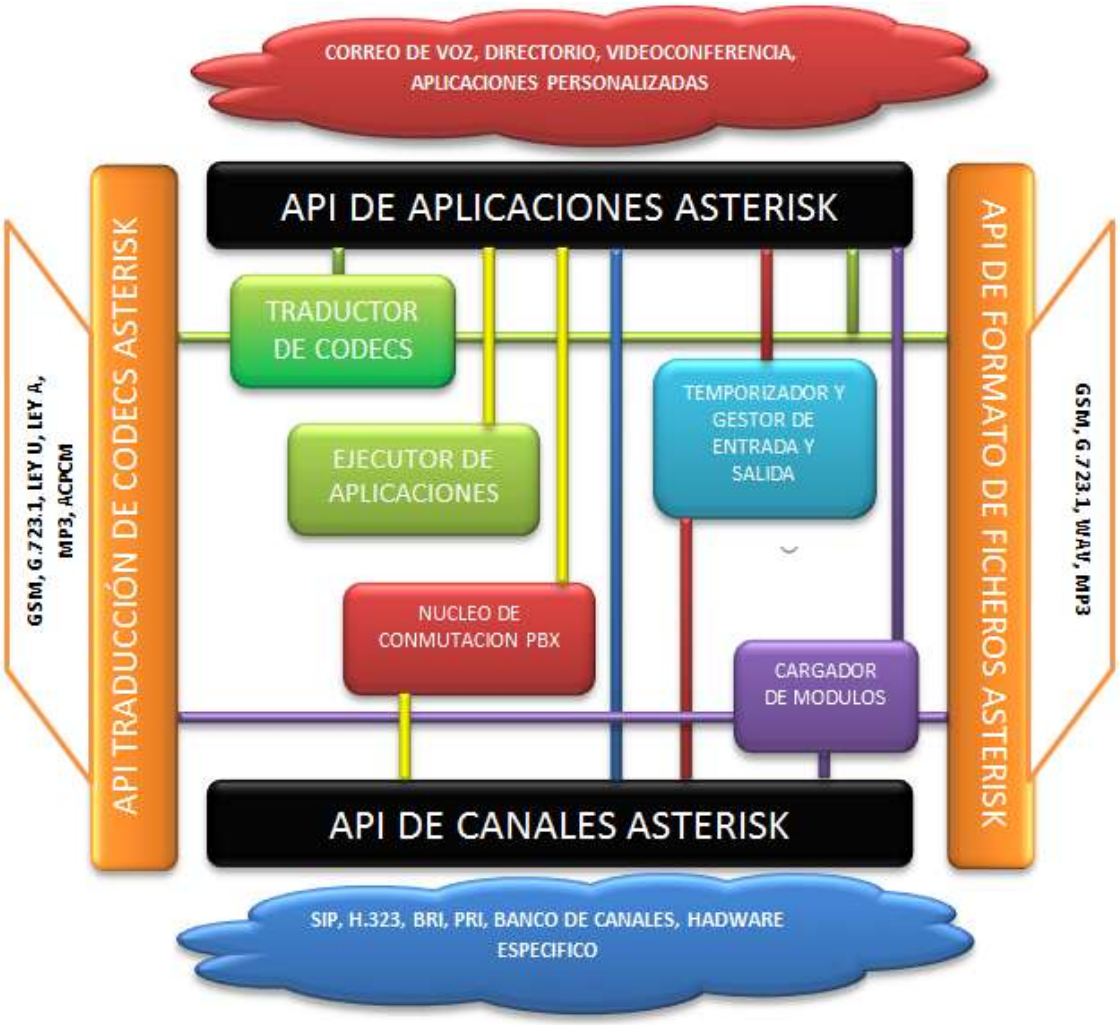


Figura No. 6.35: Arquitectura de Asterisk
Elaborado por: Freddy Robalino

Al iniciar el Cargador de Módulos Dinámicos de Asterisk, este carga e inicializa cada uno de los drivers de los diferentes canales, los formatos de los archivos, códecs, aplicaciones y más, enlazándolos con las apropiadas API internas. Esto permite al núcleo de Conmutación de la PBX Asterisk comenzar a aceptar llamadas desde las interfaces y responderlas de acuerdo con el plan de marcado, usando el ejecutor de aplicaciones. Este ejecuta aplicaciones, que a su vez realizan

servicios para los usuarios, como llamar a los teléfonos, correo de voz, reproducción de archivos, etc.

Para facilitar la abstracción de protocolos y de hardware se definen cuatro módulos que tienen la capacidad de cargar cuatro interfaces de programas de aplicación. Usando este sistema de cargar módulos, el núcleo de Asterisk no tiene que preocuparse por los detalles de cómo el llamante se ha conectado o que códecs está usando, etc.

- API para los canales, sirve para controlar todas las llamadas del sistema, sean Voz IP, analógicas cualquier otra tecnología pudiendo desarrollar nuevos canales
- La API para la Traducción de Códec, carga los módulos de códec que le permiten soportar varios formatos de codificación y decodificación de la voz como pueden ser GSM, Ley µ, Ley A, MP3. Por lo general son códecs que no requieren patentes.
- API de Formato de Ficheros, sirve para controlar el formato de ficheros que pueden ser administrados por el sistema.
- API de Aplicaciones, son herramientas desarrollados como complemento a las ya tradicionales existentes en la telefonía analógica tradicional

Asterisk posee múltiples módulos e interfaces

- El núcleo PBX interconecta llamadas entre diferentes tecnologías de hardware y software (manejadas por los módulos chan_*.so)
- El lanzador de aplicaciones, integrado con el Dial plan, ejecuta funciones como buzones de voz, música en espera (módulos App_*.so)
- El traductor de Códecs permite la traducción de diferentes formatos de compresión de audio (módulos codec_*.so)
- El Manejador de E/S permite leer y escribir la configuración de Asterisk en varios formatos (módulos res_*.so)

Características de la extensión Asterisk

Esta se define como una lista de aplicaciones y argumentos para ejecutar. Cada paso de una extensión está referido a una prioridad y ejecuta una aplicación. Cada operación en una llamada es manejada invocando una aplicación. Hay disponibles un gran número de aplicaciones para realizar varias funciones de una PBX. Las aplicaciones de Asterisk proporcionan tanto características básicas como avanzadas. Asterisk tiene aplicaciones para marcar, descolgar, responder o reproducir un archivo de sonido. Las aplicaciones más avanzadas proporcionan la creación de correos de voz, conferencia y servicios de directorio. Cada prioridad generalmente es ejecutada por orden aunque algunas aplicaciones como "Dial" y "Goto" pueden remitir una llamada a una prioridad diferente. Cada paso en una extensión, típicamente se hace como sigue.

La estructura de Asterisk permite la integración de gran parte de códecs de audio además de proveer de todas las aplicaciones de la telefonía analógica tradicional. Asterisk da paso a la creación de nuevas aplicaciones y servicios que un usuario, de la universidad y la facultad pueda requerir sobre una PBX, esto se debe a que Asterisk es creado en un ambiente de código fuente abierta. Por todo esto, Asterisk es una herramienta versátil que permite caracterizar cada una de las extensiones de forma individual.

El momento de configurar una extensión, se debe completar las características mostradas en la siguiente tabla.

CARACTERÍSTICA	FUNCIÓN
Seguridad	Permitir llamadas de larga distancia solo desde teléfonos seguros
Ruteo	Encaminar las llamadas basadas en extensiones
Contestadora	Saludar a los llamadores y preguntarles para entrar a las extensiones.
Autenticación	Preguntar por la palabra clave al entrar a las extensiones asignadas
Privacidad	Lista negra de llamadores fastidiosos
Macros	Crear aplicaciones para las funciones más comúnmente utilizadas

Tabla No. 6.11: Características de una Extensión Asterisk.
Elaborado por: Freddy Robalino

Posible Asignación Numérica a los Terminales IP

Asterisk permite extensiones de hasta 5 dígitos, pudiendo de esta manera diferenciar entre grupos de extensiones pertenecientes a una misma dependencia de la red, en su defecto, para asociar extensiones a grupos de similares funciones o características.

Para distinguir una extensión entre los campus, se utiliza una extensión de 4 dígitos, el primer digito como indicador, 1 en el caso del campus Ingahurco y 2 campus Huachi. La siguiente tabla muestra el rango de direcciones posibles.

ÁREA	PRIMER DÍGITO	RANGO DE EXTENSIONES
Ingahurco	**1**	**1001-1999**
Huachi	**2**	**2001-2999**
Remoto	**3**	**3001-3999**

Tabla No. 6.12: Numeración Campus Ingahurco.
Elaborado por: Freddy Robalino

En el caso de la red de la facultad extensión puede ser de 4 dígitos, el primer digito como indicador, 1 en el caso de la dependencia 1 y 2 en el caso de la dependencia 2. La siguiente tabla muestra el rango de posibles direcciones.

ÁREA	PRIMER DÍGITO	RANGO DE EXTENSIONES
Dependencia 1	**100**	**1000-1999**
Dependencia 2	**101**	**2000-2999**
Remoto	**102**	**3000-3999**

Tabla No. 6.13: Numeración Campus Huachi.
Elaborado por: Freddy Robalino

De esta manera se procede a asignar la numeración tomando en cuenta un aproximado de 100 posibles usuarios, y permitiendo extensiones para usuarios remotos.

Herramientas de Administración

La mayor parte de la flexibilidad de Asterisk es controlada a través de los archivos de configuración que se localizan en el directorio etc/Asterisk. La sintaxis de la configuración está diseñada de forma que le sea más fácil analizarla tanto al software, como a la persona que opera el sistema. Mediante los archivos de configuración se establecen todos los servicios que ofrece Asterisk, los canales (SIP, H.323), objeto de nuestro estudio, las interfaces y principalmente el "Plan de Marcación" que a la postre es el que va a permitir la comunicación a través de Asterisk.

El Plan de Marcación es configurado en el archivo extension.conf. La configuración de este archivo permite encaminar todas las llamadas en el sistema, desde la fuente hasta el destino final, mediante varias aplicaciones.

Asterisk permite administrar usuarios por nombre o por número de extensión, de esta manera se configura el protocolo VoIP para cada usuario, puede ser SIP o H.323, teniendo en cuenta que las extensiones se podrán comunicar únicamente si utilizan el mismo protocolo.

Para limitar el número de usuarios y garantizar la comunicación con la central telefónica se asigna una ID de usuario y una contraseña, restringiendo el acceso a usuarios no autorizados.

Asterisk cuenta con la herramienta Asterisk Logs que permite monitorear llamadas concurrentes y mantener un registro de las llamadas de cada una de las extensiones, además mostrando el protocolo utilizado, el número de extensión, dirección IP origen - destino y el tiempo de duración.

La conexión VPN propuesta en este proyecto describe un proceso de acuerdo al protocolo de seguridad utilizado. IPSec establece en 5 fases el túnel VPN, que luego se puede utilizar también para transmitir conversaciones telefónicas seguras,

para esto durante el proceso se realizan intercambios de contraseñas con sus respectivas identificaciones de usuario o de túnel, además se procede con diferentes procesos de verificación y autenticación.

Una vez establecido el túnel VPN con IPSec todos los usuarios podrán acceder a través del servidor Asterisk, que administra el tráfico y la transmisión de datos de manera segura. Los usuarios registrados en éste servidor podrán comunicarse entre ellos, independientemente de donde se encuentren. Dado que el tráfico generado se mantiene dentro de la red de la facultad.

Estudio de costos de la toda la propuesta

Tras haber culminado el diseño de la propuesta con sus respectivos procesos y con un panorama completo del alcance del presente proyecto, es posible establecer que equipos y elementos intervienen; o pueden intervenir, en la implementación y puesta en marcha de la red diseñada.

En este capítulo se realizará el estudio de costos, además se detallan los equipos necesarios para una futura implementación de todo el proyecto.

Habiendo elegido elementos gratuitos y tratando de mantener un enfoque objetivo y de menor impacto económico, se presenta como un proyecto de bajo presupuesto para la universidad y de grandes alcances tanto a nivel administrativo como económico.

Equipos necesarios para la implementación

Considerando que la institución cuenta con una red de cableado estructurado e infraestructura LAN previa, no será necesaria su estudio de costos y no se requiere de cambios en la arquitectura física como en la arquitectura lógica de la red.

Teniendo en cuenta este aspecto, se procede a detallar los equipos y elementos de software que se utilizan para este proyecto.

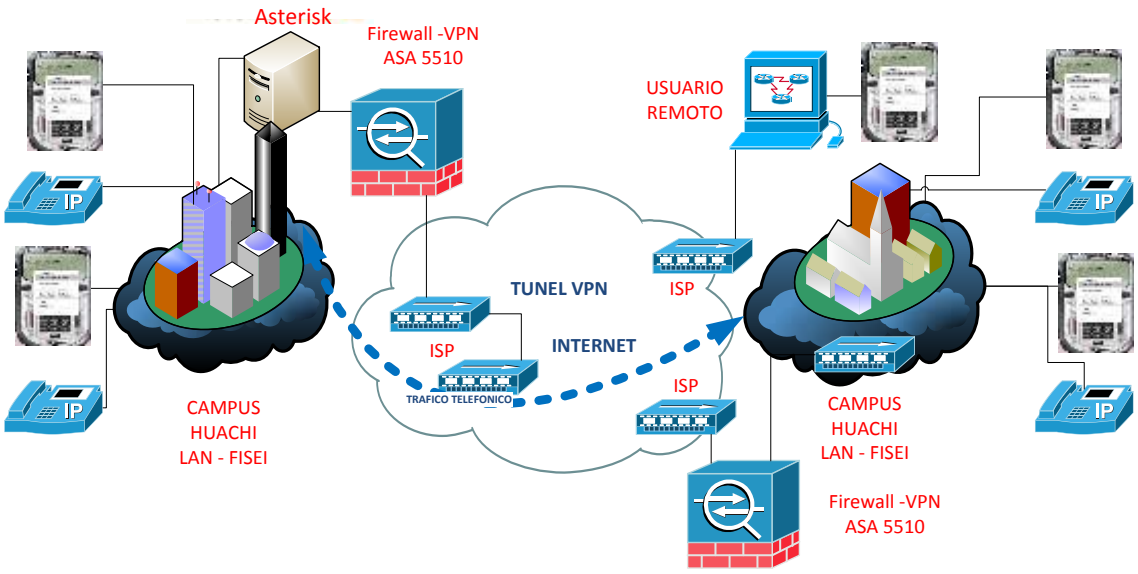


Figura No. 6.36: Esquema topológico de la red propuesta
Elaborado por: Freddy Robalino

Para una topología de Intranet VPN se requiere de 2 equipos que soporten túneles IPSec VPN y una conexión a Internet con al menos un ancho de banda de 1024 Kbps, en los dos campus, como se indicó anteriormente.

Costos

Considerando los equipos y otros elementos que interviene para la realización del presente proyecto, se diferencian 3 tipos de gastos, que se reflejan a continuación:

Costo de equipos

Los costos más importantes respecto a los equipos utilizados, son los relacionados a los equipos de borde, Firewall ASA 5510, que por las características que presta, fácilmente permite reemplazar a cualquier equipo destinado a la administración de

la red en el caso el servidor de VLANs de la Facultad o simplemente ampliar su cobertura, en cuyo caso es una inversión muy acertada.

En la siguiente tabla se indican los parámetros básicos que debe tener el equipo VPN.

CARACTERÍSTICA	NECESARIO MÍNIMO	CISCO ASA 5510
Usuarios / Nodos	200	Ilimitado
Throughput VPN 3DES/ AES	50 Mbps	Sobre los 225 Mbps
Pares VPN IPsec	50	750
Puertos de Red Integrados	1 Gigabit Ethernet, 2 Fast Ethernet	4 Gigabit Ethernet, 1 Fast Ethernet
Protocolos VPN Soportados	IPSec	IPSec, PPTP, SSL
Algoritmos de Encripción	AES (128 bits)	DES, 3DES, AES (128, 192, 256 bits)
Algoritmos de Autenticación	MD5	MD5, SHA, RSA, DSA
Protocolos de Encapsulamiento	ESP	ESP
Protocolo de establecimiento de sesión	IKE, ISAKMP	IKE, ISAKMP
Protocolo de llaves públicas	Diffie-Hellman Grupo 1 (768 bits)	Diffie-Hellman Grupo 1 (768 bits) Grupo 2 (1024 bits) Grupo 5 (1536 bits) Grupo 7 (mayor 1536 bits)

Tabla No. 6.14: Características y requisitos del equipo VPN.
Elaborado por: Freddy Robalino

Características y requisitos del equipo VPN

Si la universidad y facultad no dispone del capital necesario el cual se detalla a continuación, para la compra de equipos ASA 5510, se puede recurrir a una opción más económica, por ejemplo un equipo de la serie Cisco Routers 2600 cargado con una versión IOS[20] 12.2 o superior, que cumple con el requerimiento mínimo de administración de túneles VPN, tanto para topologías o escenarios Sitio a Sitios.

Si decidiese implementar el servidor de telefónica con asterisk, este requiere un mínimo de recursos de hardware concentrando su rendimiento sobre aplicaciones específicas. En este caso Asterisk Now está direccionado a la administración de centrales telefónicas y para ello se requiere de un equipo con las características promedio indicadas en la siguiente tabla.

CARACTERÍSTICA	MÍNIMO / NECESARIO	ÓPTIMO
Disco Duro	40 GB	160 GB
Procesador	Pentium D 3,0 GHz	Doble Núcleo 2 GHZ
Memoria RAM	512 MB	1 GB

Tabla No. 6.15: Características del servidor Asterisk Now.
Elaborado por: Freddy Robalino

Como se aclaró anteriormente si se instala el servidor Asterisk Now se estimaría un requerimiento, de al menos 10 teléfonos IP pueden ser 3COM 3101 los cuales que cumplen con el requisito necesario de soportar protocolo SIP.

En cuanto al número de teléfonos IP que se requerirían en un principio, no sería necesario facilitar un equipo de comunicación para cada punto de red en que se requiera de una extensión. En este sentido se recomienda usar el software Softphone (Para un mayor detalle ver Anexo C-Sección C.2), X-lite; que es fácil

de utilizar y no interfiere en el desempeño del host sobre el que se instala. Dicho esto a continuación se detalla el costo de implementación de equipos.

CANTIDAD	EQUIPO	USO	UBICACIÓN	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
1	Cisco ASA 5510	Administración de conexiones VPN LAN a LAN y usuarios remotos.	Campus Ingahurco	6000	6000
1	Cisco ASA 5510	Administración de conexiones VPN LAN a LAN y usuarios remotos.	Campus Huachi	6000	6000
1	Computador-Servidor Asterisk	Para soportar sistema operativo Asterisk.	Edificio FISEI	700	700
10	Teléfonos IP	Extensión telefónica	Edificio FISEI o en el campus Huachi	30	300
TOTAL SIN IMPUESTOS					13000

Tabla No. 6.16: Costo Total de Equipos.
Elaborado por: Freddy Robalino

Costos de software

El software Cliente VPN Cisco es el único software propietario que se necesitaría para la realización de este proyecto, los elementos adicionales se encuentran disponibles en diferentes sitios de Internet en forma gratuita, en el caso de ser así se ha tomado en cuenta este rubro.

Detalles del servidor Asterisk[21] mientras que
Detalles del Sofphone[22]X-lite
Detalle de los costos de software se detalla a continuación.

CANTIDAD	EQUIPO	USO	UBICACIÓN	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
1	Software Cliente VPN Cisco	Permite conexión segura entre un host y un equipo de frontera.	Equipos remotos	500	500
1	Software Asterisk Now	Administra extensiones telefónicas.	Servidor ubicado en el Edificio de la FISEI.	0	0
1	Softphone X-Lite	Emula un teléfono físico IP y se carga sobre PCs clientes	En equipos usuarios terminales en los 2 campus y usuarios remotos.	0	0
TOTAL SIN IMPUESTOS					500

Tabla No. 6.17: Costo del Software
Elaborado por: Freddy Robalino

El costo mensual que se requiere para una conexión a Internet se describe en la siguiente tabla y como se requiere el mismo ancho de banda para los dos campus.

CANTIDAD	ANCHO DE BANDA	VALOR MENSUAL (USD)	TOTAL MENSUAL (USD)
2	Conexión 1024 Kbps	75	75
1	Conexión residencial 512 Kbps	25	25
TOTAL MENSUAL SIN IMPUESTOS			**425**

Tabla No. 6.18: Costo del Servicio de Internet
Elaborado por: Freddy Robalino

Aun cuando la Universidad tiene un contrato anual de internet de con una ancho de banda actual de 28mb y a la facultad se le asigna un ancho actualmente de 3,5mb y valor de pago anual de 30000 Usd. El costo del internet se lo toma en el caso de implementarlo en una empresa o institución con recursos menores.

Costos de instalación

Los costos de configuración incluyen el periodo de pruebas que se lleve a cabo, una vez configurados los equipos, los cuáles se muestran en la siguiente tabla.

Nº DE HORAS	CONFIGURACIÓN EQUIPOS/ SOFTWARE	COSTO HORA (USD)	COSTO TOTAL (USD)
5	Router ASA 5510, campus Huachi.	100	500
3	Router ASA 5510, campus Ingahurco.	100	300
6	Central Telefónica Asterisk	60	360
10	Teléfono IP y Softphone	30	300
1	Cliente VPN Asterisk	40	40
VALOR TOTAL SIN IMPUESTOS			**1500**

Tabla No. 6.19: Costo de Configuración
Elaborado por: Freddy Robalino

En el caso del equipo ASA 5510 ubicado en el campus Huachi (FISEI) se toma en cuenta un número adicional de horas debido a que ese equipo contendrá la configuración para usuarios remotos, además del respectivo periodo de pruebas.

En el caso de la configuración de la Central telefónica Asterisk, se considera un largo tiempo debido al número de extensiones que se requiere.

Para el caso de los Teléfonos IP y Softphone, se estima un tiempo aproximado de 5 minutos por extensión, y el tiempo se justifica debido al número de extensiones que se requiera configurar.

El software Cliente VPN Cisco se instala en los PC remotos, y el costo dependerá del número de usuarios remotos que requieran.

Costos totales

Finalmente el costo total de implementación del presente propuesta se muestra en la siguiente tabla. Se toman en cuenta todas las consideraciones hechas anteriormente y no se incluyen los costos mensuales por concepto de Internet por la razón descrita anteriormente.

DESCRIPCIÓN	VALOR (DÓLARES)
Total Equipos Hardware	13000
Total Elementos Software	200
Total Configuración	1500
TOTAL SIN IMPUESTOS	14700

Tabla No. 6.20: Costo de Total de la Propuesta
Elaborado por: Freddy Robalino

Con este estudio de costos realizados se da una visión general del costo de implementación del presente proyecto con los equipos propuestos. Cabe recalcar que para la implementación del túnel VPN se pueden utilizar otros equipos más económicos, pero que no cuentan con todas las funcionalidades del equipo propuesto como el soporte de protocolos que brindan seguridad, además el costo es para toda la universidad.

Previsión de la Evaluación

La administración del servidor, equipos de frontera, y protocolos de seguridad, además sus resultados serán evaluados principalmente por el administrador de la red y el diseñador de la red respectivamente.

INDICADORES ACTIVIDAD	Semana Numero	Forma de Evaluación	Responsable
Administración del Servidor Asterisk de manera eficaz	1	Cantidad de cuentas y accesos controlados.	Administrador de Red.
Verificación de la calidad de servicio	2	Cantidad y orden de paquetes Entregados al destino.	Administrador de Red, Diseñador.
Cantidad de accesos al servicio de telefonía	3	Estadísticas de acceso en el servidor Asterisk.	Administrador de Red
Cantidad de accesos al servicio de forma remota	4	Estadísticas de acceso en el servidor Asterisk.	Administrador de Red
Utilización de normas de regulación la transmisión de información (Uso de protocolos de seguridad).	5	Conjunto de normas Aplicadas a la transmisión.	Administrador de Red
Comunicación entre el emisor y el receptor es óptima en todo momento	6	Perdida de paquetes en la comunicación.	Administrador de Red
Calidad de servicio	7	Retardo de los paquetes al llegar a su destino.	Administrador de Red
Confianza de los usuarios en el nivel de seguridad que se dan a sus datos	8	Cantidad de usuario conformes con el servicio.	Diseñador

Tabla No. 6.21: Previsión de la Evaluación
Elaborado por: Freddy Robalino

Guía de implementación de la red propuesta

Introducción

En base al diseño y a las consideraciones realizadas en el mismo, para el túnel VPN con IPsec, se describirán los pasos para la implementación, donde se incluirán las configuraciones de equipos propuestos.

1.- Consideraciones

Para el túnel VPN, de LAN a LAN, se configura el equipo de frontera en cada una de las redes LAN que se encuentran separadas por una nube WAN.

2.- Pasos para la implementación de IPSec

En el siguiente diagrama de bloques se describe los pasos a seguir, para la configuración de la VPN mediante el protocolo IPSec.

Figura No. 6.37: Diagrama de Bloques (IPSec)
Elaborado por: Freddy Robalino

2.1.- Configuración del tráfico de interés

Este es el tráfico que va a pasar el túnel VPN, y que necesita ser encriptado. En este caso son los paquetes de VoIP, ya que los paquetes de voz se enviaran a través del túnel, permitiendo realizar llamadas entre los usuarios de manera segura.

Se debe considerar como política enviar el tráfico cifrado entre las terminales VPN, y el texto plano en otras conexiones que no requieran encripción. Esta diferenciación se realiza en los equipos de frontera, la red pública (Internet), y la red privada, como se muestra a continuación.

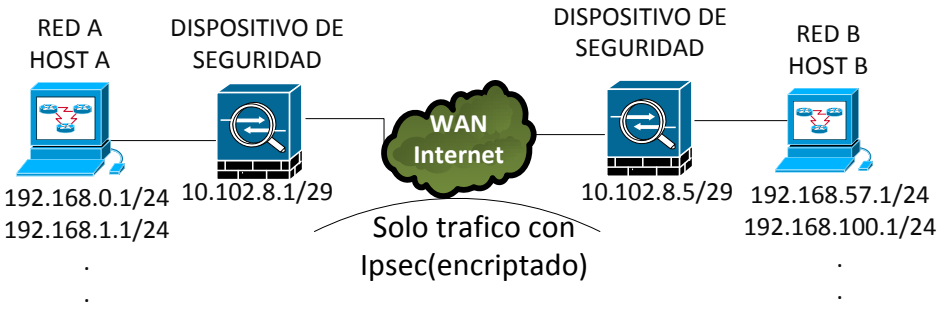


Figura No. 6.38: Trafico de Interés
Elaborado por: Freddy Robalino

Para esto se define el tráfico de interés en cada uno de los equipos ASA por medio de listas de acceso habilitando los puertos necesarios para enviar el tráfico entre los extremos del túnel.

Las listas de acceso configuradas son del tipo extendidas y tienen el siguiente formato.

Fisei1-fw1 (config)# access-list (name) (tipo de access-list) (permiso) (protocolo) (origen) (destino) eq (puerto)

En la siguiente Tabla se describe los comandos de la instrucción anterior y su respectiva descripción.

Opciones	Comando	Descripción
Name	---	Palabra o número menor a 241 caracteres
Tipo de access-list	Standard	Configura una lista de acceso del tipo estándar
	Extended	Configura una lista de acceso del tipo extendida
Permisos	Permit	Especifica los tipos de paquetes que se van a enviar
	Deny	Especifica los tipos de paquetes que se van a rechazar
Protocolo	Ip	Configura Internet Protocol
	Tcp	Configura Transmission Control Protocol
	Udp	Configura User Datagram Protocol
	Ipsec	Configura IP Security
	Icmp	Configura Internet Control Message Protocol
Origen	Hostname or A.B.C.D	Dirección o nombre del host de origen
	Any	Desde cualquier origen
	Host	Se configura un host como origen
	Interface	Usa la dirección de la interfaz como

		dirección origen
	object-group	Especifica un grupo de máquinas o redes como dirección origen
Destino	Hostname or A.B.C.D	Dirección o nombre del host de destino
	Any	Hacia cualquier destino
	Host	Se configura un host como destino
	Interface	Usa la dirección de la interfaz como dirección destino
	object-group	Especifica un grupo de máquinas o redes como dirección destino
Puerto	nombre o número de puerto	El número de puerto entre 0 y 65535

Tabla No. 6.22: Comandos Para Definir Tráfico de Interes
Elaborado por: Freddy Robalino

En nuestro caso los paquetes que requieren ser encriptados son los paquetes de voz. A continuación se tiene la configuración del protocolo SIP (puerto UDP 5060) como tráfico interesante. Estos comandos se deben configurar en cada equipo VPN.

Fisei-fw1 (config)# access-list 101 permit udp 192.168.1.1 255.255.255.0 192.168.100.1 255.255.255.0 eq 5060
Ingahurco-fw2(config)# access-list 101 permit udp 192.168.100.1 255.255.255.0 192.168.1.1 255.255.255.0 eq 5060

En caso que se requiera de otras aplicaciones, diferentes de la de voz, se puede definir como tráfico de interés los puertos requeridos (en dependencia del tipo de datos que necesite) o en su defecto a todo el conjunto de protocolos IP entre los extremos del túnel. A continuación se indica la configuración del conjunto de protocolos IP como tráfico de interés.

Fisei-fw1 (config)# access-list 101 permit ip 192.168.1.1 255.255.255.0 192.168.100.1 255.255.255.0
Fisei-fw1 (config)# nat (inside) 0 access-list 101
Ingahurco-fw2 (config)# access-list 101 permit ip 192.168.100.1 255.255.255.0 192.168.1.1 255.255.255.0
Ingahurco -fw2 (config)# nat (inside) 0 access-list 101

Otro comando que se utiliza es el "nat 0", para que las redes definidas en las listas de acceso no se traduzcan por el protocolo NAT, que normalmente se define para que las redes tengan salida a Internet, de tal manera que al acceder a la VPN las host terminales las podamos ver con las direcciones IP originales en cualquier lugar o punto del túnel.

2.2.- Políticas de Seguridad

2.2.1.- Internet key Exchange Fase 1

En este paso se configuran políticas de seguridad que se mantendrán durante la conexión del túnel VPN. Éstas deben ser iguales en los dos equipos que se utilizan para el túnel en este punto se indicara la configuración del dispositivo de seguridad que se encontrara en la facultad.

Los parámetros que se definen en la política de seguridad son los siguientes:

- Método de Autenticación
- Algoritmo de Encriptación
- Grupo DH
- Algoritmo Hash
- Lifetime (Tiempo de vida del túnel)

Los comandos que se utilizan tienen el siguiente formato:

Fisei-fw1 (config)# crypto iskmp policy (número de política) (autenticación / encripción / grupo / hash / lifetime) (opción)

En la siguiente Tabla se muestra los comandos y los parámetros de configuración.

Opciones	Comando	Subcomando	Descripción
Política	crypto isakmp policy	---	Configura las políticas con el protocolo ISAKMP
Número de política	1 – 65535	---	Prioridad de la política (1 es la más alta)
Autenticación del Peer	Authentication	pre-share	Configura clave pre-confgurada manualmente
		rsa-sig	Configura el algoritmo rsa-sig
		dsa-sig	Configura el algoritmo dsa-sig
Algoritmo de Encripción	Encryption	Des	Configura des (56 bits)
		3des	Configura 3des (168 bits)
		Aes	Configura aes (128 bits)
		aes-192	Configura aes (192 bits)
		aes-256	Configura aes (256 bits)
Grupo	Group	1	Diffie-Hellman group 1 (768 bits)
		2	Diffie-Hellman group 2 (1024 bits)
		5	Diffie-Hellman group 5 (1536 bits)
		7	Diffie-Hellman group 7 (mayor 1536 bits)
Algoritmo de	Hash	md5	Configura hash md5

Integridad de mensajes		Sha	Configura hash sha
Tiempo de vida	Lifetime	tiempo	Se escribe el tiempo de duración del túnel en segundos
		None	Se tiene un túnel con un tiempo de duración ilimitado

Tabla No. 6.23: Comandos Para Definir Políticas
Elaborado por: Freddy Robalino

A continuación para configurar pre-share, aes, group 2, md5, lifetime de 86400 segundos (1 día):

Fisei-fw1(config)# crypto isakmp policy 10 authentication pre-share
Fisei-fw1(config)# crypto isakmp policy 10 encryption aes
Fisei-fw1(config)# crypto isakmp policy 10 group 2
Fisei-fw1(config)# crypto isakmp policy 10 hash md5
Fisei-fw1(config)# crypto isakmp policy 10 lifetime 86400

2.2.1.- Internet key Exchange Fase 2

En este paso se configura el encapsulamiento de paquetes con los protocolos de encripción y de autenticación establecidos previamente en la fase 1 de IKE. Los comandos a configurar tienen el siguiente formato:

Fisei-fw1(config)# crypto ipsec transform-set (name) (encapsulamiento-protocolo)

La siguiente tabla muestra los parámetros de encapsulación que se pueden hacer.

Parámetro	Característica
Name	Palabra menor a 64 caracteres
esp-des	ESP transform using DES cipher (56 bits)
Esp-3des	ESP transform using 3DES cipher(168 bits)
esp-aes	ESP transform using AES-128 cipher
esp-aes-192	ESP transform using AES-192 cipher
esp-aes-256	ESP transform using AES-256 cipher
esp-md5-hmac	ESP transform using HMAC-MD5 auth
esp-sha-hmac	ESP transform using HMAC-SHA auth
Esp-none	ESP no authentication
Esp-null	ESP null encryption

Tabla No. 6.24: Parámetros de Encapsulamiento
Elaborado por: Freddy Robalino

Con la siguiente línea se da la configuración de la política de seguridad para la VPN en donde se encapsulan los paquetes con ESP y el algoritmo de autenticación MD5 y AES.

Fisei-fw1 (config)# crypto ipsec transform-set equipo_vpn esp-aes esp-md5-hmac

3.- Sesión IPSec

Una vez configurado todos los parámetros para el túnel IPSec, se establece la sesión IPSec para transmitir información entre los extremos del túnel.

3.1.- Finalización de la sesión del túnel

En la siguiente figura se muestra un esquema de la terminación del túnel.

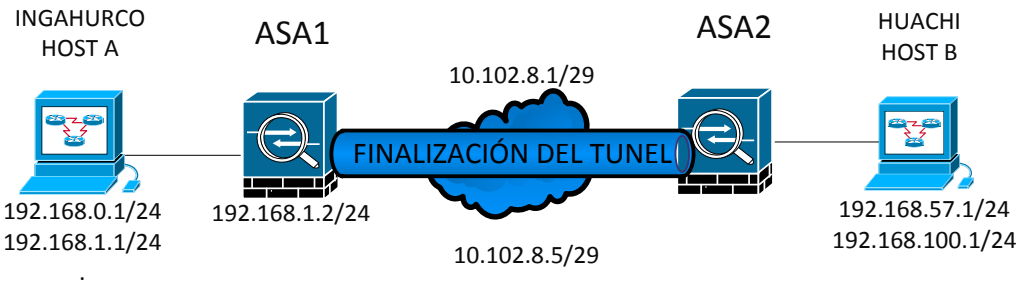


Figura No. 6.39: Finalización del Túnel
Elaborado por: Freddy Robalino

Cabe aclarar que la sesión del túnel VPN puede terminar por tres causas:

1. Por vencer el tiempo de vida o lifetime con el que fue configurado el túnel.

   Comando para configurar el tiempo de vida:
   Fisei-fw1 (config)# isakmp policy 10 lifetime (tiempo en segundos)
   El lifetime se puede configurar con un tiempo mínimo de 120 segundos hasta 2147483647 segundos que es aproximadamente a 68 años.
   Pero si desea que el tiempo de vida del túnel sea ilimitado, se puede utilizar la opción de "none".
2. El túnel no se establece, si los parámetros de los equipos de seguridad son diferentes
3. La sesión establecida se pierde, si los parámetros del equipo son removidos o se modifican.

Una vez definidos los pasos para configurar el túnel se procede a con la descripción de los escenarios propuestos y las configuraciones respectivas.

4.- Configuración VPN de Lan-to-Lan con IPSec usando equipos Cisco

Para el establecimiento del escenario VPN LAN a LAN debe tener las siguientes características:

Topología: LAN –TO- LAN

Tecnología de Túnel: IPSec

Plataforma: Por hardware usando equipos CISCO ASA serie 5510

Equipos: 2 Equipos Cisco ASA serie 5510.
2 Dos computadores Pentium D

4.1.- Escenario

Las pruebas de implementación de la VPN con IPSec y el desempeño del servicio de VoIP se realizaron en la Academia de Redes Cisco Ambato de la Facultad de Ingeniería en Sistemas, gracias a la colaboración de dicha unidad y por la prestación de los equipos ASA por la academia regional.

Figura No. 6.40: Academia de Redes CISCO-CTT-FISEI
Tomado por: Freddy Robalino

Se simulara la topología de Huachi-FISEI y la de Ingahurco enfocado en los equipos de frontera con los que se establecerá el túnel IPSec entre las dos.

En la siguiente figura se muestra la topología propuesta para la implementación del túnel VPN entre dos redes LAN.

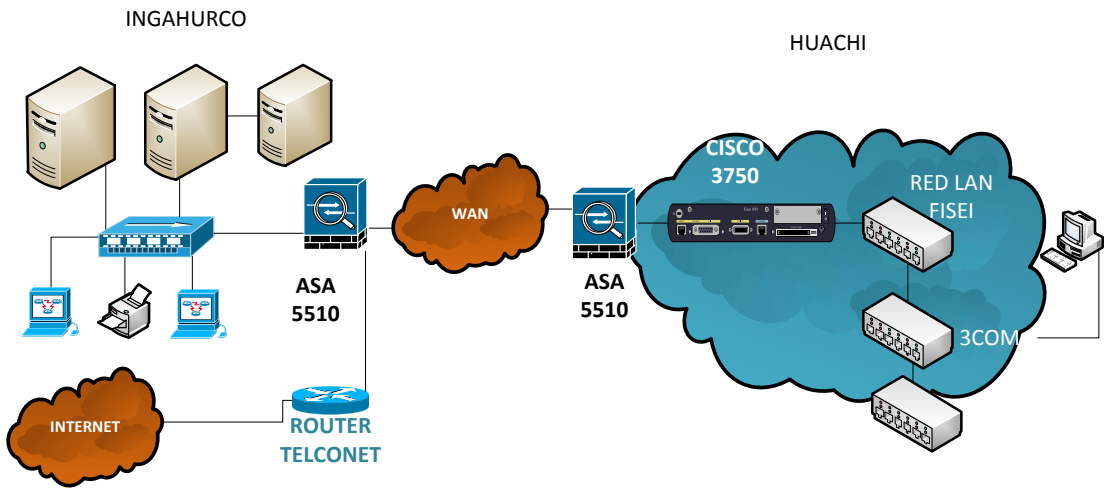


Figura No. 6.41: Red VPN con IPsec sobre la red de la UTA
Diseñado por: Freddy Robalino

4.2.- Direccionamiento de la red propuesta

Aquí se describe el direccionamiento propuesto de los equipos a utilizar para la implementación.

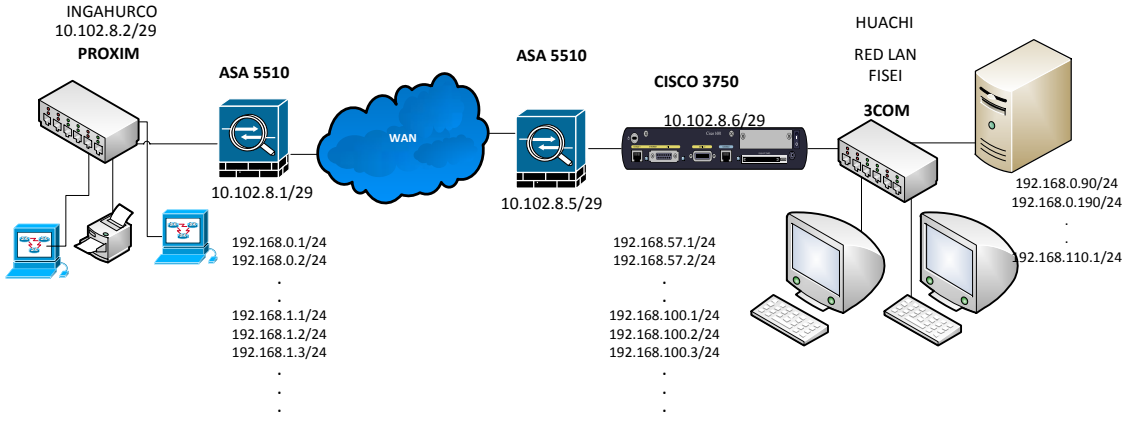


Figura No. 6.42: Diseño Implementado de una VPN LAN a LAN
Diseñado por: Freddy Robalino

4.3.- Instalación y configuración

En Ingahurco la dirección de la red luego del router Cisco del ISP (TELCONET) es 10.102.8.1 con máscara 255.255.255.0, y en el otro extremo en Huachi la dirección de red es 10.102.8.5 con máscara de 255.255.255.0
Estos equipos y la interfaz del equipo ASA se conectan a un Switch de 24 puertos (PROXIM). Por otro lado, la interfaz del otro equipo ASA en el Huachi-Fisei se conecta directamente al Switch de Core (CISCO3750).

En Ingahurco, la dirección IP de la estación de trabajo es 192.168.1.1/ 24 y en el Huachi-FISEI, la dirección IP de la estación de trabajo es 192.168.100.1/ 24 y si los administradores consideran instalar el servidor Asterisk, este se configurara con la dirección de red 192.168.110.0 / 24.

La configuración de los equipos ASA para el establecimiento de la VPN IPSec entre las dos LANs es la siguiente:

Equipo ASA-Ingahurco

Ingahurco-asa1(config)# tunnel-group 10.102.8.1 type ipsec-l2l
Ingahurco -asa1(config)# isakmp enable outside
Ingahurco -asa1(config)# isakmp identity address
Ingahurco -asa1 (config)# isakmp policy 10 encryption aes
Ingahurco -asa1(config)# isakmp policy 10 hash md5
Ingahurco -asa1(config)# isakmp policy 10 authentication pre-share
Ingahurco -asa1(config)# isakmp policy 10 group 1
Ingahurco -asa1(config)# isakmp policy 10 lifetime none
Ingahurco -asa1(config)# tunnel-group 10.102.8.1 ipsec-attributes
Ingahurco -asa1(config-tunnel-ipsec)# pre-shared-key cisco
Ingahurco -asa1(config)# access-list 101 permit ip 192.168.1.1 255.255.255.0 192.168.100.0 255.255.255.0
Ingahurco -asa1(config)# nat (inside) 0 access-list 101

Ingahurco -asa1(config)# crypto ipsec transform-set equipo_vpn esp-des esp-md5-hmac

Ingahurco -asa1(config)# crypto map ES_1_MAP 10 match address 101

Ingahurco -asa1(config)# crypto map ES_1_MAP 10 set peer 10.102.8.5

Ingahurco -asa1(config)# crypto map ES_1_MAP 10 set transform-set equipo_vpn Ingahurco -asa1 (config)# crypto map ES_1_MAP 10 set security-association lifetime seconds 48000

Ingahurco -asa1(config)# crypto map ES_1_MAP interface outside

Ingahurco -asa1(config)# route outside 0.0.0.0 0.0.0.0 10.102.8.1

Ingahurco -asa1(config)# crypto ipsec transform-set remoteuser1 esp-des esp-sha hmac Ingahurco -asa1(config)# crypto dynamic-map rmt-dyna-map 10 set transform-set remoteuser1

Ingahurco -asa1(config)# crypto map rmt-user-map 10 ipsec-isakmp dynamic rmt-dyna-map

Ingahurco -asa1(config)# crypto map rmt-user-map interface int_vpn

Equipo ASA-Huachi

Huachi –asa2 (config)# tunnel-group 10.102.8.5 type ipsec-l2l

Huachi –asa2 (config)# isakmp enable outside

Huachi –asa2 (config)# isakmp identity address

Huachi –asa2 (config)# isakmp policy 10 encryption aes

Huachi –asa2 (config)# isakmp policy 10 hash md5

Huachi –asa2 (config)# isakmp policy 10 authentication pre-share

Huachi –asa2 (config)# isakmp policy 10 group 1

Huachi –asa2 (config)# isakmp policy 10 lifetime none

Huachi –asa2 (config)# tunnel-group 10.102.8.5 ipsec-attributes

Huachi –asa2 (config-tunnel-ipsec)# pre-shared-key cisco

Huachi –asa2 (config)# access-list 101 permit ip 192.168.1.0 255.255.255.0 192.168.100.1 255.255.255.0

Huachi –asa2 (config)# nat (inside) 0 access-list 101

Huachi –asa2 (config)# crypto ipsec transform-set equipo_vpn esp-des esp-md5-hmac Huachi –asa2 (config)# crypto map ES_1_MAP 10 match address 101

Huachi –asa2 (config)# crypto map ES_1_MAP 10 set peer 10.102.8.1
Huachi –asa2 (config)# crypto map EQUIPO_1_MAP 10 set transform-set equipo_vpn Huachi –asa2 (config)# crypto map EQUIPO_1_MAP 10 set security-association lifetime seconds 48000
Huachi –asa2 (config)# crypto map EQUIPO_1_MAP interface outside
Huachi –asa2 (config)# route outside 0.0.0.0 0.0.0.0 192.168.8.5
Huachi –asa2 (config)# crypto ipsec transform-set remoteuser1 esp-des esp-sha hmac Huachi –asa2 (config)# crypto dynamic-map rmt-dyna-map 10 set transform-set remoteuser1
Huachi –asa2 (config)# crypto map rmt-user-map 10 ipsec-isakmp dynamic rmt-dyna-map
Huachi –asa2 (config)# crypto map rmt-user-map interface int_vpn

Las configuraciones para el establecimiento del túnel son las siguientes:

- Método de Autenticación: md5
- Algoritmo de Encripción: aes (128 bits)
- Grupo DH: Grupo 1 (768 bits)
- Lifetime: none (ilimitado)
- Contraseña: cisco

4.4.- Configuración de la nube WAN

La nube WAN está implementada con routers Cisco 3750. El propósito de la nube WAN es simular la red mundial de Internet, para obtener un escenario propicio para probar el diseño y configuración propuesta. Las topologías que se implementan es la siguiente:

Topología Tipo Bus Punto A Punto

En esta topología se utiliza dos routers Cisco de la serie 1841 conectados en serie y configurados para que la red 10.102.8.1/29, Ingahurco, tenga conectividad con la red 10.102.8.5/29, Huachi.
Resumen de los parámetros configurados en los ruteadores.

Ítem	Router1	Router2
Nombre de Host	Router1	Router2
Contraseña de la consola	Cisco	Cisco
Contraseña vty	Cisco	Cisco
Int Fa 0/0	192.168.1.2 / 24	192.168.100.2 / 24
Int Fa 0/1	10.102.8.1 / 29	10.102.8.5 / 29
Protocolo de enrutamiento	OSPF	OSPF
Descripción Interfaz fa 0/0	Puerta de enlace ASA1	Puerta de enlace Huachi – asa2
Descripción Interfaz fa 0/1	Conexión con Router2	Conexión con Router1

Tabla No. 6.25: Topología Tipo Bus: Configuración De Routers
Elaborado por: Freddy Robalino

5.- Pruebas y Evaluación de Seguridad

Para las pruebas de seguridad que proporciona el túnel VPN con IPSec se debe monitorear el túnel para determinar la encripción de los datos que se transmiten a través de él, esto se lo hará con la herramienta Wireshark (Para una guía de uso e instalación Ver. ANEXO E).

El monitoreo se lo realiza con un host-local y un host-intruso, para comparar los resultados y determinar la encripción de los paquetes. El host-intruso se conecta con una ip de cualquiera de las subredes que se necesite de Lan para el host-local a través de un hub, se utiliza este dispositivo ya que por concepción este

dispositivo retransmite la información a todos los puertos (broadcast), permitiendo la evaluación y monitoreo de la red desde algún otro host este caso el intruso, simulando lo que haría un hacker desde algún punto sobre la gran nube de Internet (WAN). La topología se indica en la siguiente figura.

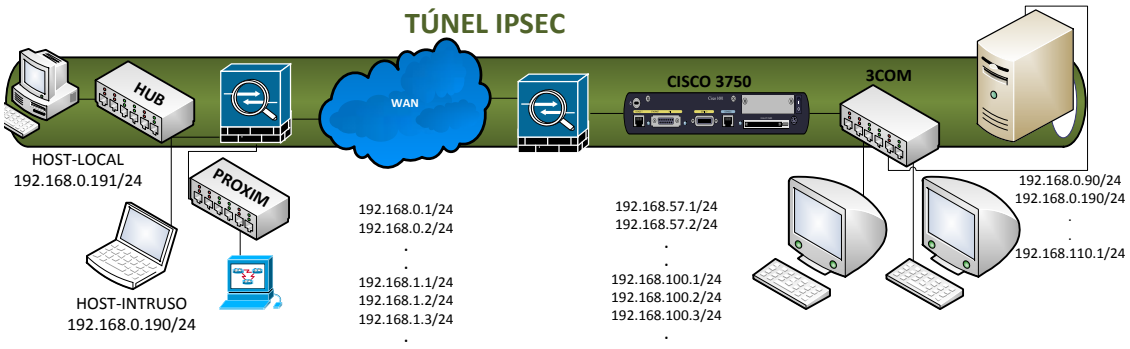


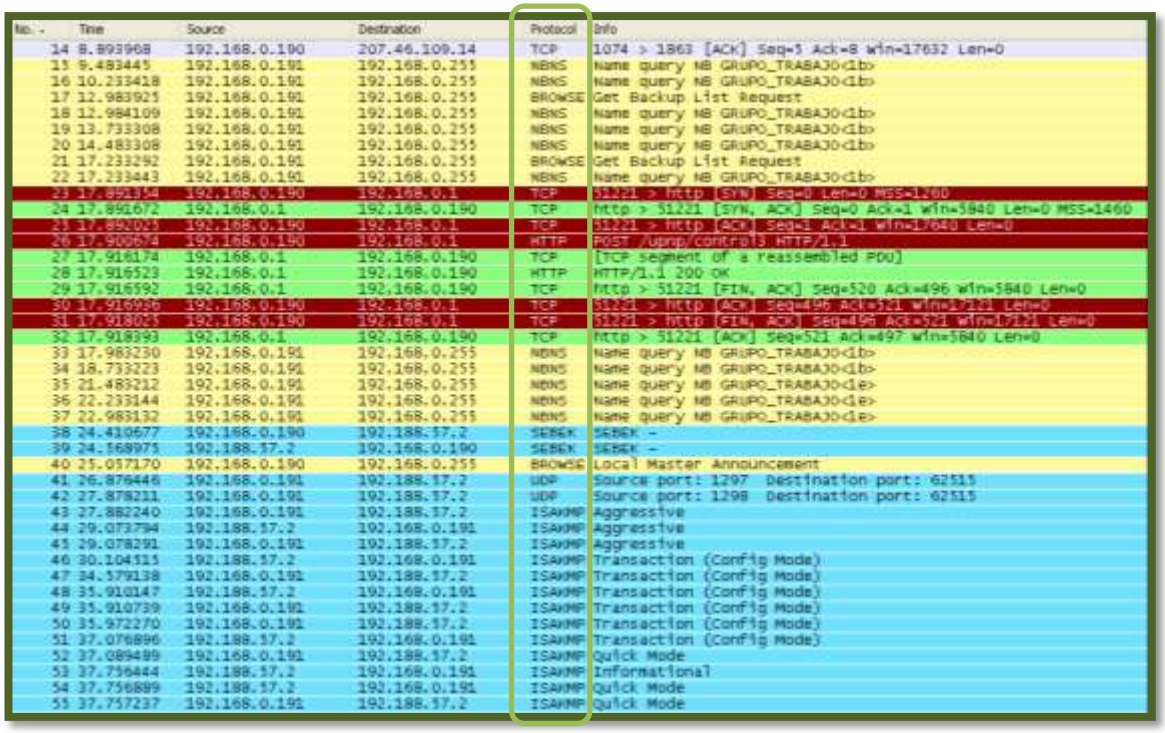
Figura No. 6.42: Túnel IPSec Topología Tipo Bus

Diseñado por: Freddy Robalino

Antes de establecer el túnel, el host-local y el host-intruso, podrán ver los datos que el host-local está transmitiendo. El host-local establece la sesión del túnel, luego de lo cual transmite datos a través del mismo (puede ser llamada telefónica, sesión VoIP con hardware o software). Los protocolos de encriptación a nivel local son transparentes para el usuario, es decir que el monitoreo realizado muestra los protocolos utilizados por los paquetes de datos de las aplicaciones del usuario, como por ejemplo TCP, HTTP, UDP, SIP, etc.

Pero luego de cargar o iniciar la configuración en los equipos de seguridad, el host-intruso, solo podrá ver los paquetes transmitidos por el host-local como paquetes ESP, indistintamente del contenido del paquete; es decir, mientras el host-local transmite paquetes TCP, HTTP, UDP, SIP, el host-intruso solo puede ver paquetes ESP (Encapsulated Security Payload), el cual forma parte de la arquitectura de seguridad del protocolo de Internet (IPSec), proporcionando así integridad, autenticación y cifrado para los datagramas del protocolo de Internet (IP) y del servicio de VoIP.

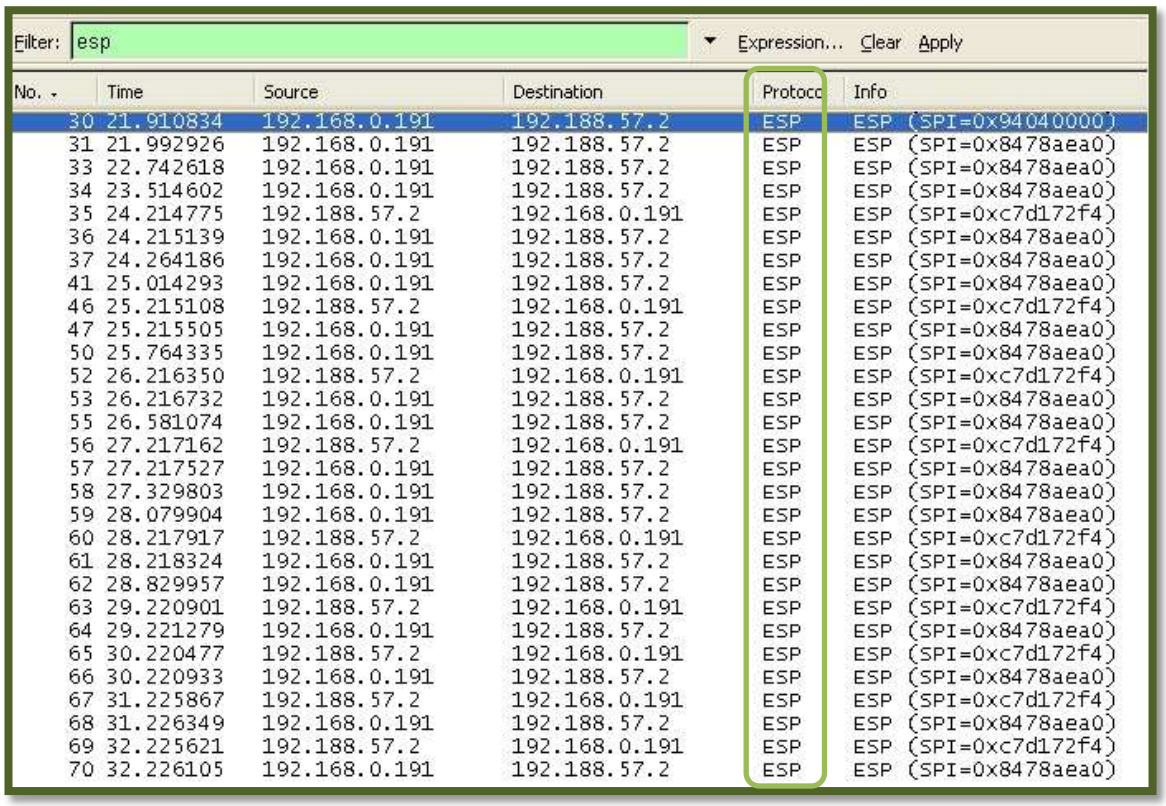
Esto se indica en las siguientes figuras respectivamente.



No.	Time	Source	Destination	Protocol	Info
14	8.893968	192.168.0.190	207.46.109.14	TCP	1074 > 1863 [ACK] Seq=5 Ack=8 Win=17632 Len=0
15	9.483445	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
16	10.233418	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
17	12.983921	192.168.0.191	192.168.0.255	BROWSE	Get Backup List Request
18	12.984109	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
19	13.733308	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
20	14.483308	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
21	17.233292	192.168.0.191	192.168.0.255	BROWSE	Get Backup List Request
22	17.233443	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
23	17.892154	192.168.0.190	192.168.0.1	TCP	51721 > http [SYN] Seq=0 Len=0 MSS=1460
24	17.896672	192.168.0.1	192.168.0.190	TCP	http > 51221 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	17.896963	192.168.0.190	192.168.0.1	TCP	51221 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
26	17.900674	192.168.0.190	192.168.0.1	HTTP	POST /upnp/control3 HTTP/1.1
27	17.916174	192.168.0.1	192.168.0.190	TCP	[TCP segment of a reassembled PDU]
28	17.916523	192.168.0.1	192.168.0.190	HTTP	HTTP/1.1 200 OK
29	17.916592	192.168.0.1	192.168.0.190	TCP	http > 51221 [FIN, ACK] Seq=520 Ack=496 Win=5840 Len=0
30	17.916956	192.168.0.190	192.168.0.1	TCP	51721 > http [ACK] Seq=496 Ack=521 Win=17121 Len=0
31	17.918043	192.168.0.190	192.168.0.1	TCP	51721 > http [FIN, ACK] Seq=496 Ack=521 Win=17121 Len=0
32	17.918393	192.168.0.1	192.168.0.190	TCP	http > 51221 [ACK] Seq=521 Ack=497 Win=5840 Len=0
33	17.983230	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
34	18.733223	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1b>
35	21.483212	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1e>
36	22.233144	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1e>
37	22.983132	192.168.0.191	192.168.0.255	NBNS	Name query NB GRUPO_TRABAJO<1e>
38	24.410677	192.168.0.190	192.188.57.2	SEBEK	SEBEK -
39	24.569971	192.188.57.2	192.168.0.190	SEBEK	SEBEK -
40	25.057170	192.168.0.190	192.168.0.255	BROWSE	Local Master Announcement
41	26.876446	192.168.0.191	192.188.57.2	UDP	Source port: 1297 Destination port: 62515
42	27.878211	192.168.0.191	192.188.57.2	UDP	Source port: 1298 Destination port: 62515
43	27.882240	192.168.0.191	192.188.57.2	ISAKMP	Aggressive
44	29.073794	192.188.57.2	192.168.0.191	ISAKMP	Aggressive
45	29.078291	192.168.0.191	192.188.57.2	ISAKMP	Aggressive
46	30.104511	192.188.57.2	192.168.0.191	ISAKMP	Transaction (Config Mode)
47	34.579138	192.168.0.191	192.188.57.2	ISAKMP	Transaction (Config Mode)
48	35.910147	192.188.57.2	192.168.0.191	ISAKMP	Transaction (Config Mode)
49	35.910739	192.168.0.191	192.188.57.2	ISAKMP	Transaction (Config Mode)
50	35.972270	192.168.0.191	192.188.57.2	ISAKMP	Transaction (Config Mode)
51	37.076896	192.188.57.2	192.168.0.191	ISAKMP	Transaction (Config Mode)
52	37.089489	192.168.0.191	192.188.57.2	ISAKMP	Quick Mode
53	37.756444	192.188.57.2	192.168.0.191	ISAKMP	Informational
54	37.756899	192.188.57.2	192.168.0.191	ISAKMP	Quick Mode
55	37.757237	192.168.0.191	192.188.57.2	ISAKMP	Quick Mode

Figura No. 6.43: Transmisión de datos sin seguridad.

Elaborado por: Freddy Robalino



Filter: esp — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
30	21.910834	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x94040000)
31	21.992926	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
33	22.742618	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
34	23.514602	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
35	24.214775	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
36	24.215139	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
37	24.264186	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
41	25.014293	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
46	25.215108	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
47	25.215505	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
50	25.764335	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
52	26.216350	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
53	26.216732	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
55	26.581074	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
56	27.217162	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
57	27.217527	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
58	27.329803	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
59	28.079904	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
60	28.217917	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
61	28.218324	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
62	28.829957	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
63	29.220901	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
64	29.221279	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
65	30.220477	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
66	30.220933	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
67	31.225867	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
68	31.226349	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)
69	32.225621	192.188.57.2	192.168.0.191	ESP	ESP (SPI=0xc7d172f4)
70	32.226105	192.168.0.191	192.188.57.2	ESP	ESP (SPI=0x8478aea0)

Figura No. 6.44: Transmisión de datos seguros.

Luego de realizar las pruebas y analizar los resultados obtenidos, se demuestra que el establecimiento del túnel VPN con (IPSec) brinda seguridad a la transmisión de datos de VoIP entre usuarios LAN.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Las redes privadas virtuales incrementan significativamente la seguridad de los datos entre sitios que se encuentran geográficamente separadas y aún más si estas tienen protocolos seguros como IPSec a diferencia de los enlaces WAN que presentan vulnerabilidades debido a que no utilizan métodos para asegurar la transmisión de datos. Por lo tanto se puede concluir que el uso de VPNs con IPSec es conveniente.

- El establecimiento de un túnel VPN con IPsec se puede tornar difícil si no se establecen reglas técnicas de configuración, ya que se debe tomar en cuenta el tráfico que se debe encriptar para túnel y las asociaciones de seguridad para el protocolo.

- Se debe considerar como política enviar el tráfico cifrado entre las terminales VPN, y el texto plano en otras conexiones que no requieran encripción. Esta diferenciación se debe realizar en los equipos de frontera, la red pública (Internet-WAN), y la red privada (LAN), esto debe estar claro en los pasos para el establecimiento de una sesión VPN con IPSec.

- La captura de paquetes hecha por el software Wireshark, permite distinguir los protocolos utilizados por el usuario local (host-local) dentro del túnel VPN, como TCP, UDP, SIP, etc. Pero cuando se monitorea desde un PC externo (host-intruso), conectado al mismo dominio que el usuario local, el

tráfico se encripta e identifica como ESP[24]. De esta manera se demuestra que el tráfico que sale del usuario se transmite de forma encriptada.

- Las ventajas de la telefonía ip administradas por servidores linux radica inicialmente en sus bajos costos operativos y de instalación ya que utiliza la misma red para transmisión de datos y voz, con soporte H.323 y SIP en donde el ultimo toma ventaja de los protocolos de VoIP existentes para manejar cierta partes del proceso

- Entre los servicios adicionales que se pueden brindar a través del túnel se está el servicio de escritorio remoto, tele-trabajadores, video conferencia, compartición de recursos como documentos e impresoras, etc.

Recomendaciones

- Una vez implementada la VPN con IPSec, se recomienda brindar servicios adicionales aprovechando el túnel establecido, por lo que la presente propuesta se limita a brindar seguridad a los datos.

- Se sugiere que las contraseñas tengan un periodo corto de duración y el administrador del túnel las cambie periódicamente, de esta manera se evita que algún usuario no autorizado acceda al túnel.

- Se recomienda que el servicio de VoIP se encuentre dentro de las políticas de tráfico de interés de la facultad, brindando prioridad al tráfico de VoIP por necesitar ser transmitido en tiempo real.

- Para empresas que no cuenten con una central analógica PBX, pero que cuenten con una red LAN estructurada, se recomienda implementar una central telefónica digital mediante Asterisk NOW, optimizando la red existente.

- Antes de decidir implementar el servicio de VoIP se debe calcular el ancho de banda adicional que se necesita incrementar, para el servicio de VoIP para evitar la saturación del canal.

BIBLIOGRAFÍA

Libros

Beltrao Moura, José Antao, Redes Locales De Computadoras, Protocolos De Alto Nivel Y Evaluación De Las Prestaciones, Editorial: Mcgraw-Hill

Gonzales Sainz, Néstor, COMUNICACIONES Y REDES DE PROCESAMIENTO DE DATOS, Editorial: McGraw-Hill, C1987

Huidrovo, José Manuel, REDES DE COMUNICACIÓN, Editorial: Paraninfo - España

Madron, Thomas M, REDES DE ÁREA LOCAL: LA SIGUIENTE GENERACIÓN, Editorial: México: Megabyte: Grupo Noriega, MÉXICO

Hopper, Andrew, DISEÑO DE REDES LOCALES, Editorial: Argentina: Addison Wesley Iberoamericana.

Tanenbaum Andrew, REDES DE COMPUTADORAS, Editorial: Prentice-Hall

Forouzan Behrouz A., TRANSMISIÓN DE DATOS Y REDES DE COMUNICACIÓN, Editorial: McGraw-Hill

Nichols, Randall K, SEGURIDAD PARA COMUNICACIONES INALÁMBRICAS: REDES, PROTOCOLOS, CRIPTOGRAFÍA Y SOLUCIONES, Editorial: McGraw-Hill Interamericana de España

León-García Alberto, REDES DE COMUNICACIÓN, CONCEPTOS FUNDAMENTALES, Editorial: McGraw-Hill / Interamericana de España, S.A.

García Tomas Jesús, BANDA ANCHA, Editorial: McGraw-Hill

Microsoft, DICCIONARIO DE INTERNET Y REDES, Editorial: McGraw-Hill / Interamericana de España, S.A.

Vladimirov, Andrew A, HACKING WIRELESS: SEGURIDAD DE REDES INALÁMBRICAS, Editorial: Anaya Multimedia

Carracedo Gallardo, Justo, SEGURIDAD EN REDES TELEMÁTICAS, Editorial: McGraw-Hill / Interamericana de España, S.A.

García Tomas Jesús, ALTA VELOCIDAD Y CALIDAD DE SERVICIOS EN REDES IP, Editorial: Ra-Ma

Stallings, William, COMUNICACIONES Y REDES DE COMPUTADORES, Editorial: Prentice Hall.

Navarro Schlegel, Anna, DICCIONARIO DE TÉRMINOS DE COMUNICACIONES Y REDES, Editorial: Prentice Hall

Mason, Andrew G, REDES PRIVADAS VIRTUALES DE CISCO SECURE, Editorial: PEARSON

Millán Tejedor, Ramón Jesús, DOMINE LAS REDES P2P "PEER TO PEER" Editorial: ALFAOMEGA

Douglas Comer, David L. (2000), INTERCONECTIVIDAD DE REDES CON TCP/IP VOL.2. Diseño e Implantación, Editorial: Sequent Corporation

Cisco Press (2005), FUNDAMENTOS DE SEGURIDAD DE REDES, Editorial: Academia de Networking de Cisco Systems.

Vineet Kumar, Markku Korpi y Senthil Sengodan. (2001), IP Telephony with H.323: Architectures for Unified Networks and Integrated Services, Editorial: John Wiley & Sons

Alan B. Johnston, (Enero 2001), SIP: Understanding the Session Initiation Protocol, Editorial: Artech House.

Iván Pepelma (2002), ARQUITECTURAS MPLS Y VPN – CP, EDICIÓN: 1ª, Editorial: Academia de Networking de Cisco Systems.

Enlaces

Vega Lebrún Carlos, (Enero 2009), REDES DE COMUNICACIÓN DE DATOS, Extraído el 01 de Enero del 2010 de: http://www.eumed.net/libros/2008a/348/Redes%20de%20comunicacion%20de%20datos.htm

Tella Llop, José Manuel: *Fundamentos del TCP/IP*. Publicado originalmente en septiembre de 1999 en los grupos de noticias microsoft.public.es.windows98. [TCP/IP orientado a Windows], extraído el 01 de Enero del 2010 de: http://www.saulo.net/pub/tcpip/b.htm#3-3

3CX (2009), Protocolos en la Telefonía IP, Protocolos VoIP, Extraído el 03 de Enero del 2010 de: http://www.voipforo.com/protocolosvoip.php

Osmosis Latina, (Actualizado: 2005/11/03 19:39), La Voz sobre I.P, Extraído el 08 de Enero del 2010 de:

http://www.osmosislatina.com/conectividad/voip.htm

VOIP Protocolo H.323, (Martes, 21 de abril de 2009), VOIP Protocolo H.323, Extraído el 19 de Febrero del 2010 de:
http://www.redesyseguridad.es/voip-protocolo-h323/
Manuel Benet, (3 de Marzo de 2008, 1:02 pm), Funcionamiento básico del protocolo SIP, Extraído el 25 de Febrero del 2010 de:
http://www.securityartwork.es/2008/03/03/voip-protocolo-sip/

Wikipedia, (19 abr 2010, a las 13:00), Protocolo de tiempo Real, Extraído el 15 de febrero del 2010 de:
http://sistema-voip.com.ar/protocolos-voip-protocols/

Leonel Munguía, (miércoles, abril 18, 2007), Wireshark - Filtros de Captura, Extraído el 27 de Febrero del 2010 de:
http://www.soportederedes.com/2007/04/wireshark-101-filtros-de-captura-parte.html

Rubén Cheng. (Última modificación 4 de Abril de 2005), Análisis de Protocolo, Extraído el 07 de Marzo del 2010 de:
http://ruben.cheng-ca.com/es/knowledge/network/trafficanalysis.htm

Kioskea, (16 de octubre de 2008, 15:43:31), Ataque por denegación de servicio, Extraído el 19 de Abril del 2010 de:
http://es.kioskea.net/contents/attaques/dos.php3

Admin, (10 de June, 2009), PROTOCOLOS DE SEÑALIZACIÓN IP, Extraído el 22 de Mayo del 2010 de:
http://tutorialesredesvozip.com/protocolos-de-senalizacion-ip/

RFC 4573 Traducción al español, (Julio 2006), Extraído el 26 de Mayo del 2010 de:
http://www.normes-internet.com/normes.php?rfc=rfc4573&lang=es

Wikipedia, (25 mayo 2010, a las 21:17), Session Initiation Protocol, Extraído el 22 de Mayo del 2010 de:
http://es.wikipedia.org/wiki/Session_Initiation_Protocol

José Luis Bosque (19 mayo 2006) Algoritmos de Equilibrio de Carga de Trabajo, Extraído el 12 de Noviembre del 2010 de:
http://dac.escet.urjc.es/docencia/Doctorado/CPBC/sesion5.pdf

José Ramón Esteban Martí
http://www.seguridadenlared.org/es/index25esp.html

REFERENCIAS

[1] **H.323** Es una recomendación del ITU-T, que define los protocolos para proveer Sesiones de comunicación audiovisual sobre paquetes de red.

[2] **SIP** Es un protocolo para la iniciación, modificación y finalización de sesiones De voz.

[3] **TI** Tecnologías de la información.

[4] **BSI** Es la Oficina Federal Alemana para la Seguridad de la Información.

[5] **Skype** http://www.skype.com/intl/es-es/support/user-guides/voip/

[6] **Vonage** http://www.vonage.com/how_vonage_works/

[7] **RTPC** www.ingenierias.uanl.mx/1/pdf/redes_telefonicas.pdf

[8] **Anti-IDS** http://www.sans.org/detection/anti-ids-tools-tactics_339

[9] **WAV** Es un formato de audio digital normalmente sin compresión de datos Desarrollado y Propiedad de Microsoft y de IBM que se utiliza para Almacenar sonidos en el PC

[10] **VoIP phishing** http://www.blogantivirus.com/voip-phishing-vishing

[11] **VoD** http://www.networkworld.es/Video-bajo-demanda/articulo-133120

[12] **Celdas** http://www.prteducativo.com/jovenes/comofuncionan.htm

[13] **FTP** Es un protocolo de red para la transferencia de archivos entre sistemas Conectados a una Red.

[14] **ICMP** Es un sub protocolo de control y notificación de errores del (IP). Como tal, se usa para enviar mensajes de error.

[15] **UDP** Es un protocolo del nivel de transporte basado en el intercambio de Datagramas. Permite el envío de datagramas a través de la red sin que se Haya establecido previamente una conexión.

[16] **IETF** http://www.ietf.org/

[17] **Elastix** http://www.elastix.org/
http://blogs.elastix.org/es/2009/11/30/69/
http://www.elastix.org/es/component/asterisk-vs-elastix.html

[18] **QoS** (Calidad de Servicio).Son las tecnologías que garantizan la transmisión de cierta Cantidad de información en un tiempo dado (*throughput*).

[19] **Broadcast** http://www.telematica1.unlugar.com/UNIDAD_4.htm

[20] **IOS** Sistemas Operativo del Router

[21] **Servidores Asterisk** http://www.asterisk.org/asterisknow/

[22] **Softphone X-Lite** http://www.counterpath.com/x-lite.html

[23] **NAT** http://www.josechu.com/xavi_conf/hacer_nat.htm

[24] **ESP** Proporciona servicios de autenticación y de integridad de datos mediante el cálculo e inclusión de una función hash basada en una clave para cada paquete.

GLOSARIO DE TÉRMINOS

ATM Asynchronous Transfer Mode (Modo de Transferencia Asíncrona)

CTI Computer Telephony Integration (Integración Ordenador-Telefonía)

DIFFSERV Differentiated Services Internet QoS model (modelo de Calidad de Servicio en Internet basado en Servicios Diferenciados)

DNS Domain Name System (Sistema de Nombres de Dominio)

E.164 Recomendación de la ITU-T para la numeración telefónica, especialmente para ISDN, BISDN y SMDS.

ENUM Telephone Number Mapping (Integración de Números de Teléfono en DNS)

FDM Frequency Division Multiplexing (Multiplexado por División de Frecuencia)

H.323 Estándar de la ITU-T para voz y videoconferencia interactiva en tiempo real en redes de área local, LAN, e Internet.

IETF Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)

IGMP Internet Group Management Protocol (Protocolo de Gestión de Grupos en Internet)

IN Intelligent Network (Red Inteligente)

IntServ Integrated Services Internet QoS model (modelo de Calidad de Servicio en Servicios Integrados de Internet)

IP Internet Protocol (Protocolo Internet)

IP Multicast Extensión del Protocolo Internet para dar soporte a comunicaciones multidifusión

IPBX Internet Protocol Private Branch Exchange (Centralita Privada basada en IP)

IPSec IP Security (Protocolo de Seguridad IP)

ISDN Integrated Services Data Network (Red Digital de Servicios Integrados, RDSI)

ISP Internet Service Provider (Proveedor de Servicios Internet, PSI)

ITSP Internet Telephony Service Provider (Proveedor de Servicios de Telefonía Internet, PSTI)

ITU-T International Telecommunications Union -Telecommunications (Unión Internacional de Telecomunicaciones - Telecomunicaciones)

LDP Label Distribution Protocol (Protocolo de Distribución de Etiquetas)

MCU Multipoint Control Unit (Unidad de Control Multipunto)

MGCP Media Gateway Control Protocol (Protocolo de Control de Pasarela de Medios)

MOS Mean Opinion Score (Nota Media de Resultado de Opinión)

SDP Session Description Protocol (Protocolo de Descripción de Sesión)

SIP Session Initiation Protocol (Protocolo de Inicio de Sesión)

SLA Service Level Agreement (Acuerdo de Nivel de Servicio)

SS7 Signalling System Number 7 (Sistemas de Señales número 7)

STMR Side Tone Masking Rating (Índice de Enmascaramiento para el Efecto Local)

TCP Transmission Control Protocol (Protocolo de Control de Transmisión)

TDM Time Division Multiplexing (Multiplexado por División de Tiempo)

UDP User Datagram Protocol (Protocolo de Datagramas de Usuario)

UMTS Universal Mobile Telephone System (Sistema Universal de Telecomunicaciones Móviles)

VLAN Virtual Local Area Network (Red de Área Local Virtual)

VPN Virtual Private Network (Red Privada Virtual)

xDSL Cualquiera de las tecnologías de Líneas de Suscripción Digital (por ejemplo, ADSL)

MPLS Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo)

PBX Private Branch Exchange (Centralita Telefónica Privada)

PHB Per Hop Behaviour (Comportamiento por Salto)

PoP Point of Presence (Punto de Presencia)

POTS Plain Old Telephone Service (Servicio Telefónico Tradicional)

PPP Point to Point Protocol (Protocolo Punto a Punto)

PSTN Public Switched Telephone Network (Red de Telefonía Conmutada Pública)

QoS Quality of Service (Calidad de Servicio)

RAS Registration, Authentication and Status (Registro, Autentificación y Estado)

RSVP Reservation Protocol (Protocolo de Reserva)

RTCP Real Time Control Protocol (Protocolo de Control de Tiempo Real)

RTP Real Time Protocol (Protocolo de Tiempo Real)

CODEC (codec). Algoritmo software usado para comprimir/ descomprimir señales de voz o audio. Se caracterizan por varios parámetros como la cantidad de bits, el tamaño de la trama (frame), los retardos de proceso, etc.

TRACERT es un utilitario del conjunto de protocolos TCP/IP que determina la ruta tomada, determinando el número de nodos que atraviesa un paquete desde su origen hasta su destino

RADIUS (Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

SDP, Sesión Description Protocol se usa para la negociación de las capacidades de los participantes, tipo codificación.

EXTRANET (extranet). Red que permite a una empresa compartir información contenida en su Intranet con otras empresas y con sus clientes. Las extranet transmiten información a través de Internet y por ello incorporan mecanismos de seguridad para proteger los datos.

GATEKEEPER (portero). Entidad de red H.323 que proporciona traducción de direcciones y controla el acceso a la red de los terminales, pasarelas y MCUs H.323. Puede proporcionar otros servicios como la localización de pasarelas.

GATEWAY (pasarela). Dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una otra. En **VoIP** existen dos tipos principales de pasarelas: la Pasarela de Medios (Media Gateways), para la conversión de datos (voz), y la Pasarela de Señalización (Signalling Gateway), para convertir información de señalización.

INTRANET (intranet). Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

IP TELEPHONY (Telefonía Internet). Ver «Voice over IP» jitter (variación de retardo). Es un término que se refiere al nivel de variación de retado que introduce una red. Una red con variación 0 tarda exactamente lo mismo en transferir cada paquete de información, mientras que una red con variación de retardo alta tarda mucho más tiempo en entregar algunos paquetes que en entregar otros. La variación de retardo es importante cuando se envía audio o video, que deben llegar a intervalos regulares si se quieren evitar desajustes o sonidos ininteligibles.

PACKET SWITCHING (conmutación de paquetes). Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío. A continuación, cada paquete se transmite de forma individual y puede incluso seguir rutas diferentes hasta su destino. Una vez que los paquetes llegan a éste se agrupan para reconstruir el mensaje original.

ROUTER (encaminador, enrutador). Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Es el nodo básico de una red IP.

SOFTSWITCH (conmutación por software). Programa que realiza las funciones de un conmutador telefónico y sustituye a éste al emular muchas de sus funciones de dirigir el tráfico de voz, pero además añade la flexibilidad y las prestaciones propias del tráfico de paquetes.

VoIP, Voice over IP (Voz sobre IP). Método de envío de voz por redes de conmutación de paquetes utilizando TCP/IP, tales como Internet.

ANEXOS

Anexo A

Opnet IT Gurú Edición Académica.

En este manual se pretende mostrar los fundamentos básicos del uso de OPNET IT Gurú Edición académica y de esta manera entender mejor los conceptos principales de las redes de computadores, y enfrentarse de manera eficiente a la administración y resolución de problemas que podemos encontrar en redes reales.

Descripción

OPNET IT Gurú proporciona un entorno virtual de red que modela el comportamiento de una red por completo, incluyendo sus pasarelas (routers), conmutadores (switchs), protocolos, servidores y aplicaciones en red. Con estos elementos permite diagnosticar problemas de una forma eficiente, validar cambios en la red antes de implementarlos y prever el comportamiento de la red ante futuros escenarios como crecimiento de tráfico, fallos de red, etc.
El módulo de OPNET "Aplicación para la Caracterización del Entorno" (Application Characterization Environment, ACE) permite a las empresas identificar de raíz problemas existentes en las prestaciones de las aplicaciones en red, y resolver estos problemas de manera eficiente y con bajo coste.

Requerimientos del sistema

- ✓ Intel Pentium III, 4 o compatible (500 Mhz o más)
- ✓ 256 MB de memoria RAM
- ✓ 400 MB de espacio en disco
- ✓ Pantalla: 1024 x 768 o mayor resolución, 256 colores o más
- ✓ Windows NT, Windows 2000 or Windows XP (con Service Pack 1)

Pasos para la instalación

Arrancar OPNET IT Gurú Edición Académica
Dar clic en Inicio → Programas → OPNET IT Gurú Academic Edition x.x → OPNET IT Gurú Academia Edition, donde x.x es la versión del programa (por ejemplo, 9.1).

Lee el texto sobre la licencia, y si está de acuerdo, presiones un Click en I have read this SOFTWARE AGREEMENT and I understand and accept the terms and conditions described herein.

Aparecerá la ventana de inicio de OPNET IT Gurú Edición Académica, tal y como se muestra aquí:

Comprobar las preferencias de OPNET

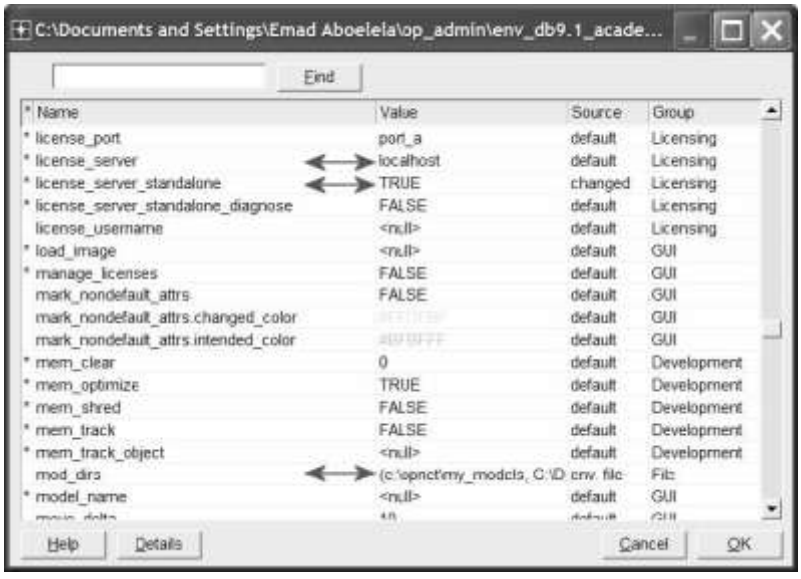
Las preferencias en OPNET permiten visualizar y editar atributos de entorno que controlan las operaciones del programa.
Después de arrancar OPNET, selecciona Preferences desde el menú Edit.
La lista de atributos de entorno está ordenada alfabéticamente, según su nombre. Se pueden localizar atributos de manera más rápida al teclear parte del nombre del atributo dentro del campo Find.

Comprueba el valor del atributo license_server, que debe corresponderse con el nombre del host desde el que se obtiene la licencia. Si IT Gurú obtiene directamente la licencia del ordenador en el que fue instalado, este valor debería de ser localhost.

Si el atributo license_server_standalone es FALSE, modifícalo a TRUE. Este atributo especifica si el programa actúa como su propio servidor de licencias.

El directorio de modelos (model directory) es un directorio que contiene los ficheros de modelos de OPNET. Si existe el atributo mod_dirs, OPNET usará los modelos que se encuentren en ese directorio. Comprueba el valor de este atributo.

El primer directorio de la lista indica dónde se guardarán tus propios modelos. En el futuro, tendrás que acceder a ese directorio para realizar copias de seguridad, o copiar y guardar tus modelos para disponer de ellos en otras prácticas. IT Gurú guarda numerosos ficheros por cada uno de los proyectos que se crean.
Da clic en OK para cerrar la ventana de diálogo.



Introducción a OPNET IT Gurú Edición Académica

Esta pequeña introducción le servirá de ayuda para empezar a usarlo.

Sobre los modelos

Los modelos estándar de IT Gurú cubren los protocolos y dispositivos comerciales más habituales. Los modelos se encuentran en los subdirectorios del directorio en el que se instaló OPNET:

<reldir>\models\std\<protocol_name>

<reldir> describe el directorio que contiene el software IT Gurú. Se puede localizar su directorio <reldir> eligiendo Help > About This Application, y mirando en OPNET root directory, dentro de la sección de información sobre el sistema.

El directorio <reldir> que se sugiere es C:\Archivos de Programa\OPNET EDU\<release_number>

Los directorios que están dentro de tutorial_req contienen los modelos que nos van a hacer falta para los tutoriales. Estos directorios tienen la siguiente forma

<reldir>\models\std\tutorial_req

El directorio tutorial_ref

<reldir>\models\tutorial_ref\itguru

Contiene versiones completas de cada uno de los modelos

Sobre IT Gurú

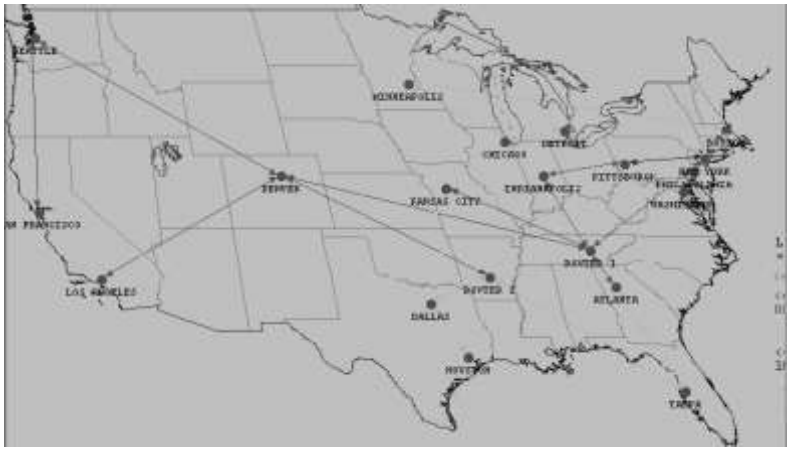
El flujo de trabajo de IT Gurú es la descripción de pasos que se usara para construir un modelo de red y ejecutar simulaciones. Este flujo de trabajo se centra alrededor del Editor de Proyectos (Project Editor).

En este editor se pueden crear modelos de red, seleccionar estadísticas de los distintos objetos o de la simulación entera, y visualizar los resultados.

Editor de Proyectos (Project Editor)

El Editor de Proyectos es el principal escenario para crear una simulación de red. A partir de este editor se puede construir un modelo de red (utilizando modelos de la librería estándar), seleccionar las estadísticas a recoger, ejecutar la simulación y ver los resultados.

Un modelo de red en el Editor de Proyectos

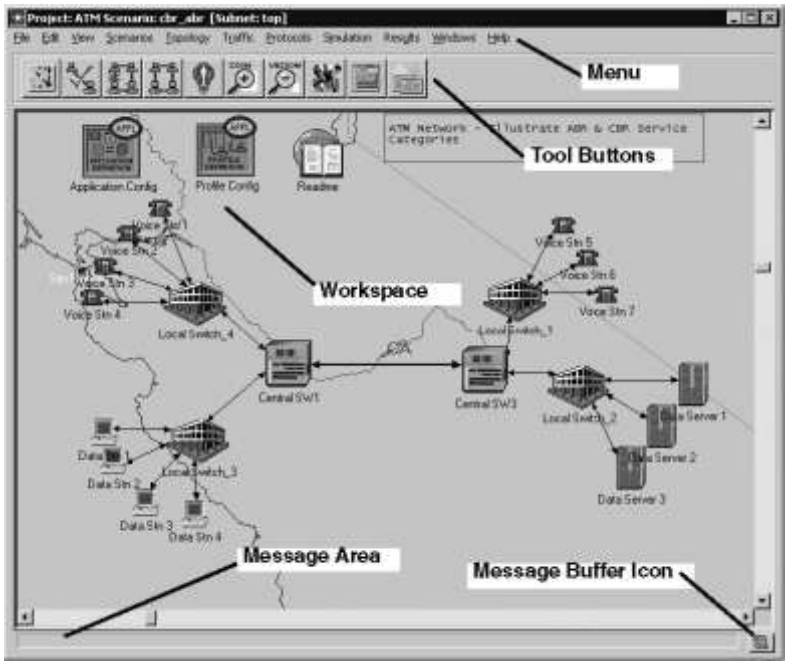


Ventana del Editor de Proyectos

Hay varias zonas en la ventana del Editor de Proyectos que son importantes para construir y ejecutar modelos. Estas zonas se muestran a continuación.

Cuando abre un proyecto que ya existe, la ventana debería mostrar algo parecido a la siguiente figura.

Ventana del Editor de Proyectos



La barra del Menú (Menú Bar)

La barra del menú se encuentra en la parte superior de la ventana de edición. Esta barra organiza todas las operaciones que no son "sensibles al contexto" mediante una estructura típica de menús.

Las operaciones "sensible al contexto" están disponibles presionando el botón derecho del ratón sobre un objeto o sobre el fondo del espacio de trabajo.

Botones de Herramientas (Tool Buttons)

Algunas de las opciones más habituales del menú también pueden ser activadas mediante los botones de herramientas. Los siguientes botones aparecen en el Editor de Proyectos: Botones del Editor de Proyectos

1 Abrir la paleta de objetos

2 Comprobar consistencia de un enlace

3 Objetos que no han sido seleccionados

4 Recuperar los objetos seleccionados

5 Volver a la subred superior (parent subnet)

6 Zoom

7 Restablecer

8 Configurar un evento discreto de simulación

9 Ver resultados de simulación

10 Esconder o ver todos los graficos.

El Área de Trabajo (Workspace)

La región central y desplazable de la ventana del editor es el área de trabajo. Los modelos de red aparecen en esta área, donde se pueden seleccionar y arrastra objetos de red, y seleccionar opciones de los menús "sensibles al contexto", al dar clic con el botón derecho sobre el fondo.

El Área de Mensajes

Esta zona se sitúa justo debajo de la ventana de edición, proporcionando información sobre el estado de la herramienta.

Se puede presionar un clic sobre el icono que hay junto a esta área de mensajes (message buffer icon), para abrir una ventana con un buffer de mensajes. Este buffer de mensajes muestra una lista de todos los mensajes que han aparecido en el área de mensajes.

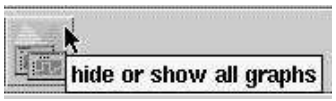
Tooltips

Si dejas el puntero del ratón sobre un botón de herramientas o un objeto de la red del área de trabajo, aparece un mensaje de ayuda. Este tooltip describe una de las siguientes cosas:

- ✓ La acción que ocurre si se pulsa el botón

- ✓ Información sobre el objeto de la red

Tooltip



Creación de la Red

Los modelos de red se crean en el Editor de Proyectos, usando nodos (node) y enlaces (link) a partir la paleta de objetos.

Nodo

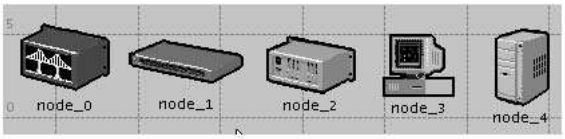
Una representación de un objeto de una red real, que puede transmitir y recibir información.

Enlace

Un medio físico de comunicación que conecta nodos entre ellos. Los enlaces representan cables eléctricos o de fibra óptica.

Estos objetos se encuentran en la paleta de objetos, que es simplemente una ventana que contiene la representación gráfica de distintos modelos de nodos y enlaces.

Nodos



Enlaces

Podemos usar tres métodos para crear una topología de red, o una combinación de estos tres. Uno de los métodos es importar la topología (lo veremos en otra práctica). Otro es situar nodos individualmente desde la paleta de objetos en la

zona de trabajo. El tercer método es usar una Configuración Rápida (Rapid Configuration).

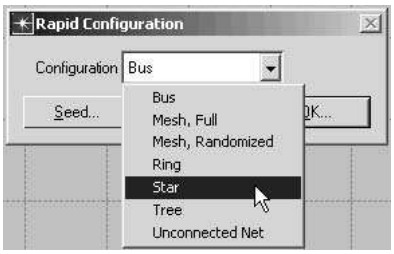
La Configuración Rápida crea toda la red con sólo una acción. Para esto, primero se selecciona una configuración de red, después los tipos de nodos de esta red y finalmente el tipo de enlace que conectan estos nodos.

Para crear la red del primer piso utilizando Configuración Rápida:

Selecciona Topology > Rapid Configuration

Selecciona Star a partir del menú desplegable disponible en la configuración, y presiona click en OK…

Configuraciones disponibles en el menú desplegable



A continuación hay que especificar los modelos de nodos y enlaces de la red. Los modelos tienen un nombre que siguen este esquema:

<protocolo1> _..._ <protocolon> _ <función> _ <mod>

dónde:

- <protocolo> especifica los protocolos específicos soportados por el modelo
- <función> es una abreviatura de "función general del modelo"
- <mod> indica el nivel de derivación del modelo

Los modelos comerciales tienen un prefijo adicional que especifica el vendedor y el número de producto para ese objeto de red.

Recoger Estadísticas

Podemos recoger estadísticas de los nodos individuales de la red (object statistics) o de la red entera (global statistics).

Luego de que hemos creado la red, deberíamos decidir qué estadísticas tenemos que recoger y responder las preguntas que se han presentado.

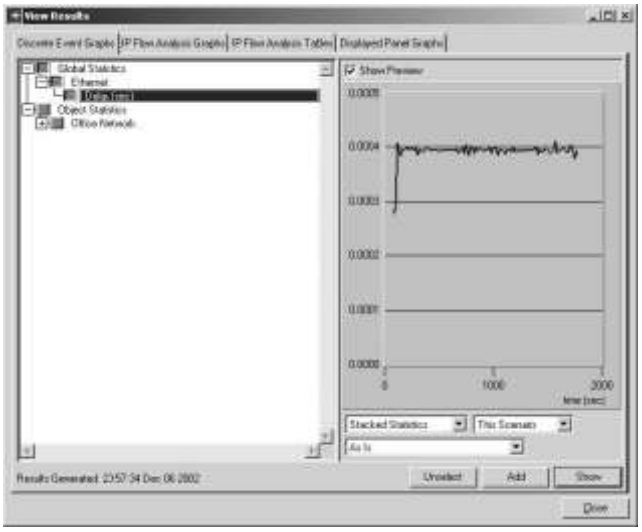
- ¿Será el servidor capaz de manejar la carga adicional de la segunda red?
- ¿Será aceptable el retardo total que exista en la red una vez que la segunda red esté instalada?

Para responder a estas cuestiones, se necesitará conocer las prestaciones actuales de la red para luego poder compararlas. La carga del servidor (Server Load) es una estadística clave que refleja las prestaciones de la red entera.

Las estadísticas globales se pueden utilizar para recoger información sobre la red como un todo.
Visualizar los Resultados

Se pueden ver los resultados de manera gráfica en el Editor de Proyectos, simplemente seleccionando View Results del menú desplegable del espacio de trabajo.
Después de haber ejecutado la simulación, querremos poder ver la información estadística que se ha recogido. Hay varias formas de ver los resultados, usando la opción View Results del menú desplegable del espacio de trabajo.

Ventana sobre el retardo de Ethernet para toda la red

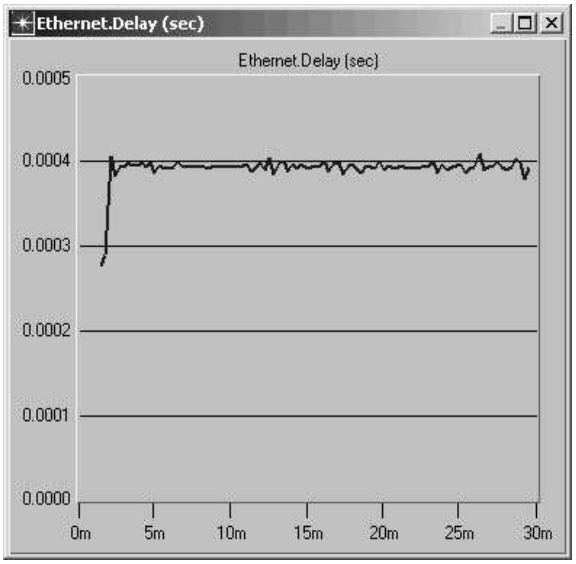


El grafico sobre el retardo de Ethernet aparece en el Editor de Proyectos. Este debería de parecerse en el siguiente gráfico.

Gráfica del retardo de Ethernet

Seconds

Simulation time, in minutes



Expansión de la Red

Hemos creado la red base y recogido estadísticas sobre su funcionamiento. Además se puede expandir la red y verificar que, pese a añadir carga adicional, la red aun funciona suficientemente bien.

Anexo B

Equipos de Seguridad y VPNs

Firewall Cisco ASA 5510

Información principal

Descripción del producto	Cisco ASA 5510 Firewall Edition - aparato de seguridad
Tipo de dispositivo	Aparato de seguridad
Tipo incluido	Montable en bastidor - 1U
Dimensiones (Ancho x Profundidad x Altura)	44.5 cm x 33.5 cm x 4.4 cm
Peso	9.1 kg
RAM instalada (máx.)	256 MB
Memoria flash instalada (máx.)	64 MB Flash
Cantidad de puertos	3
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Características	Protección firewall, asistencia técnica VPN, soporte VLAN
Alimentación	CA 120/230 V (50/60 Hz)

Especificaciones ampliadas

	Aparato de seguridad
Altura (unidades de bastidor)	1U
Cantidad de módulos instalados (máx.)	0 (1)
Anchura	44.5 cm
Profundidad	33.5 cm
Altura	4.4 cm
Peso	9.1 kg

Procesador / Memoria / Almacenamiento

RAM instalada (máx.)	256 MB
Memoria flash instalada (máx.)	64 MB Flash

Conexión de redes

Factor de forma	Montable en bastidor
Cantidad de puertos	3
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Rendimiento	Capacidad del cortafuegos : 300 Mbps
	Tasa de conexiones : 6000 sesiones por segundo

	Capacidad de la VPN : 170 Mbps
Capacidad	Peers VPN IPSec : 250
	Peers VPN SSL : 2
	Sesiones concurrentes : 50000
	Interfaces virtuales (VLAN) : 50
Cantidad de túneles VPN	50 túneles
Características	Protección firewall, asistencia técnica VPN, soporte VLAN
Algoritmo de cifrado	DES, Triple DES, AES

Expansión / Conectividad

Total ranuras de expansión (libres)	1 (1) x Ranura de expansión
Interfaces	3 x red - Ethernet 10Base-T/100Base-TX - RJ-45
	1 x gestión - Ethernet 10Base-T/100Base-TX - RJ-45
	1 x gestión - consola - RJ-45
	1 x serial - auxiliar - RJ-45
	2 x Hi-Speed USB - 4 PIN USB tipo A

Diverso

Cumplimiento de normas	CE, certificado FCC Clase A, CISPR 22 Class A, EN 60950, EN 61000-3-2, UL 1950,
	VCCI Class A ITE, IEC 60950, EN 61000-3-3, CSA 22.2 No. 950, EN55022 Class A,
	ACA TS001, AS/NZS 3260, FCC Part 15

Alimentación

Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)
Potencia suministrada	190 vatios

Parámetros de Entorno

Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 - 95%

Accesorios

Dispositivos de alimentación y UPS

ASA-180W-PWR-AC= Cisco - Fuente de alimentación (interna) - CA 100-240 V - 180 vatios

Accesorios del sistema

ASA5500-SSL-100= Cisco ASA 5500 Series SSL VPN license - Licencia - 100 usuarios

ASA5500-SSL-250= Cisco ASA 5500 Series SSL VPN license - Licencia - 250 usuarios

ASA5500-SSL-10= Cisco ASA 5500 Series SSL VPN license - Licencia - 10 usuarios

ASA5500-SSL-50= Cisco ASA 5500 Series SSL VPN license - Licencia - 50 usuarios

ASA5500-SSL-25= Cisco ASA 5500 Series SSL VPN license - Licencia - 25 usuarios

ASA5510-SEC-PL= Cisco ASA 5510 Security Plus - Licencia - 150 peers VPN

Memoria programable

ASA5500-CF-256MB= Cisco - Tarjeta de memoria flash - 256 MB - CompactFlash Card

ASA5500-CF-512MB= Cisco - Tarjeta de memoria flash - 512 MB - CompactFlash Card

Dispositivos de red

ASA-SSM-CSC-20-K9= Cisco ASA CSC-SSM-20 - Aparato de seguridad - módulo de inserción

ASA-SSM-CSC-10-K9= Cisco ASA CSC-SSM-10 - Aparato de seguridad - módulo de inserción

ASA-SSM-AIP-20-K9= Cisco ASA 5500 Series Advanced Inspection and Prevention Security
Services Module 20 - Aparato de seguridad -
Fast EN, Gigabit EN - módulo de inserción

ASA-SSM-AIP-10-K9= Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module 10 - Aparato de seguridad -
Fast EN, Gigabit EN - módulo de inserción

Adaptadores de red

SSM-4GE= Cisco Security Services Module - Módulo de expansión - EN, Fast EN, Gigabit EN - 10Base-T, 100Base-TX,
1000Base-T - 4 puertos

Accesorios de red

ASA5500-HW= Cisco Hardware Accessory Kit - Kit de accesorios para dispositivo de red

Servicio y mantenimiento de red

CON-SNTP-AS1BUNK9 Cisco SMARTnet Premium - Ampliación de la garantía - repuesto - 1 año - 24 horas diarias / 7 días semanales - 4 h
CON-SNT-AS1BUNK9 Cisco SMARTnet - Ampliación de la garantía - repuesto - 1 año - 8x5 - SDL

Aplicaciones
ASA-CSC20-USR-1K= Cisco ASA 5500 Content Security License - Licencia de actualización - 1000 usuarios - actualización de 500 usuarios
ASA-CSC20-PLUS= Cisco ASA 5500 Content Security Plus License - Licencia - 1 dispositivo
ASA-CSC10-USR-100 Cisco ASA 5500 Content Security License - Licencia de actualización - 100 usuarios - actualización de 50 usuarios
ASA-CSC10-PLUS Cisco ASA 5500 Content Security Plus License - Licencia - 1 dispositivo
ASA-CSC20-USR-750= Cisco ASA 5500 Content Security License - Licencia de actualización - 750 usuarios - actualización de 500 usuarios
ASA-CSC10-USR-250= Cisco ASA 5500 Content Security License - Licencia de actualización - 250 usuarios - actualización de 50 usuarios
ASA-CSC10-USR-100= Cisco ASA 5500 Content Security License - Licencia de actualización - 100 usuarios - actualización de 50 usuarios
ASA-SW-UPGRADE= Cisco ASA 5500 - Licencia de actualización - 1 aparato

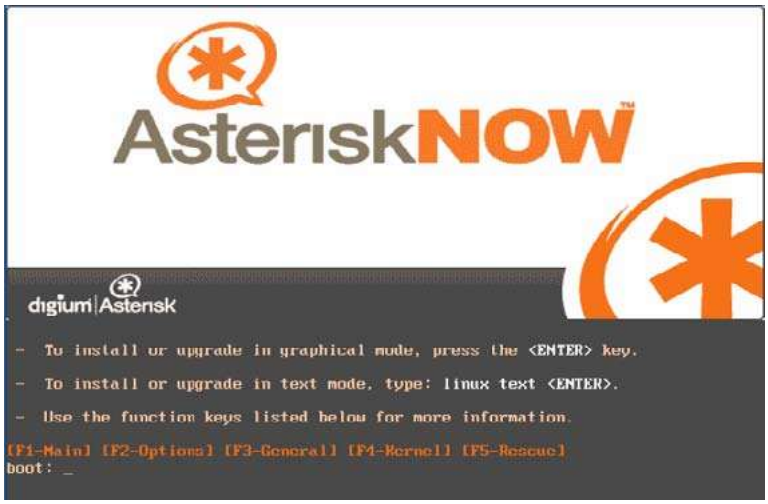
Anexo C

Configuración Asterisk NOW

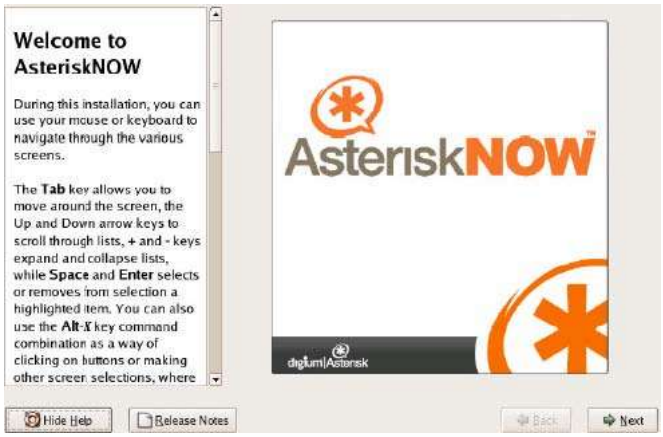
Sección C.1

Lo primero que debemos hacer es obtener una versión de Asterisk Now, se puede descargar de http: //www.asterisknow.org/, se trata de una distribución de Linux adaptada para hacer funcionar Asterisk en cuestión de minutos ya que viene con

todos los requerimientos y dependencias de software pre configurados y permite la administración y mantenimiento del servidor de una manera realmente sencilla.
Si arrancamos el PC, con el CD introducido no saldrá una primera pantalla



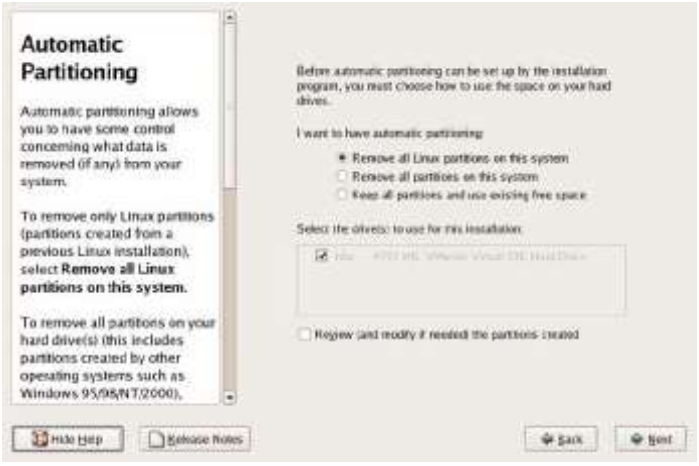
Donde pulsaremos Enter para hacer la instalación en modo gráfico. Nos saldrá una pantalla dándonos la bienvenida a la instalación.



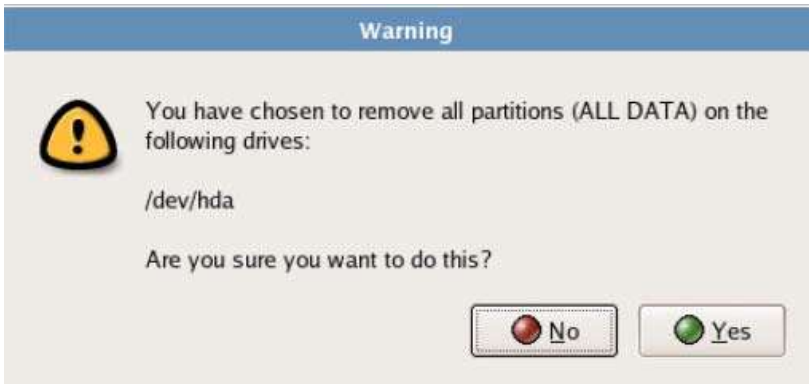
Donde deberemos pulsar el botón Next. Saldrá la siguiente pantalla, donde seleccionaremos la opción de Express installation y pulsamos Next

La siguiente pantalla puede variar. Si en el disco donde deseamos realizar la instalación de Asterisk Now, existe la instalación de un Windows, nos saldrá un mensaje indicando que se borraran todos los datos. Donde deberemos pulsar yes.

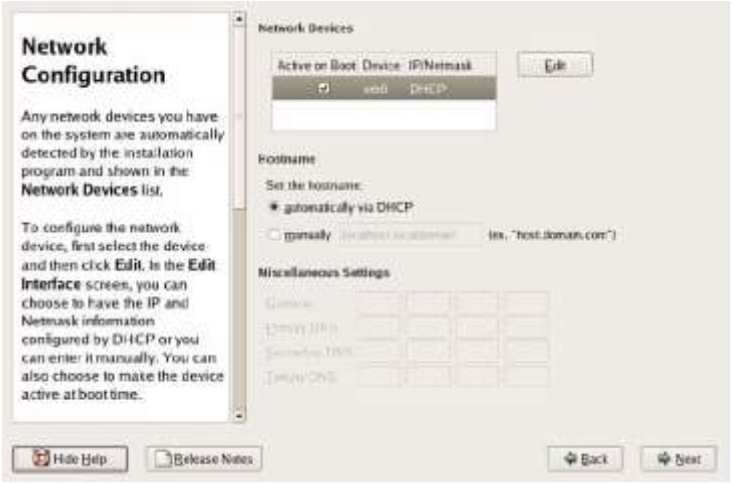
Ahora empezara el proceso de partición automático. Donde dependiendo de nuestro caso deberemos seleccionar la primera o segunda opción, y pulsar next.



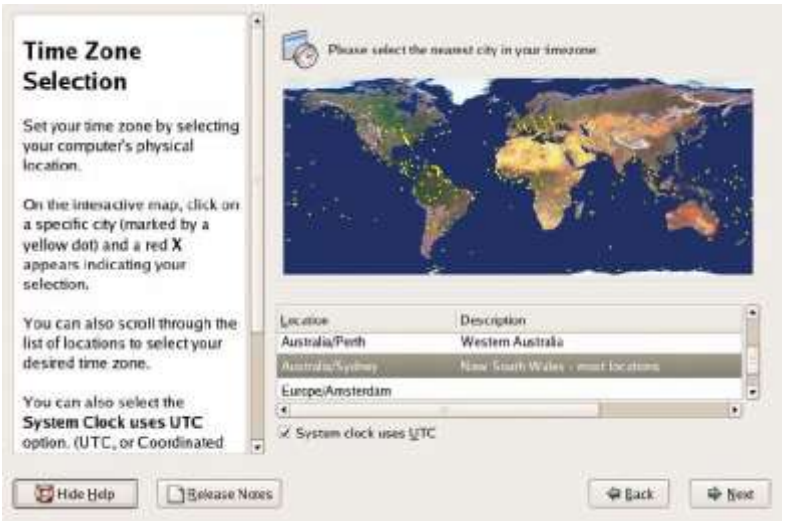
Antes de empezar el proceso de instalación, saldrá un mensaje indicando que si está seguro de eliminar las particiones. Donde pulsamos yes.



La siguiente pantalla es para configurar la red en nuestro servidor Asterisk. Donde se puede configurar mediante DHCP (obtención automática de datos) o manualmente.



La siguiente pantalla es para configurar la zona de tiempo.

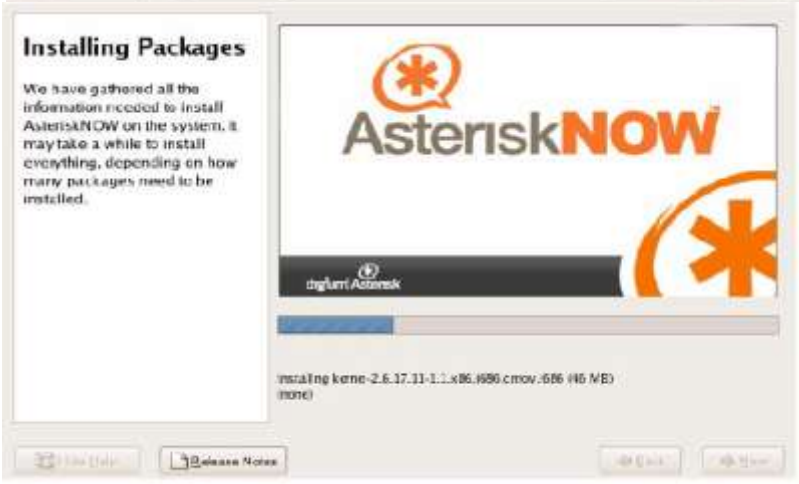


Por defecto se crea un usuario que se llama ADMIN, donde en la siguiente pantalla nos solicita la contraseña. Este será el administrador de la parte del asterisk, pero también existe el usuario ROOT que es el administrador de todo. Y pulsamos next.

Antes de comenzar la instalación, nos muestra una pantalla que nos indica procesos que se llevan a cabo en la instalación. Pulsamos next.

Antes de realizar la instalación, se debe realizar el formateo del sistema.

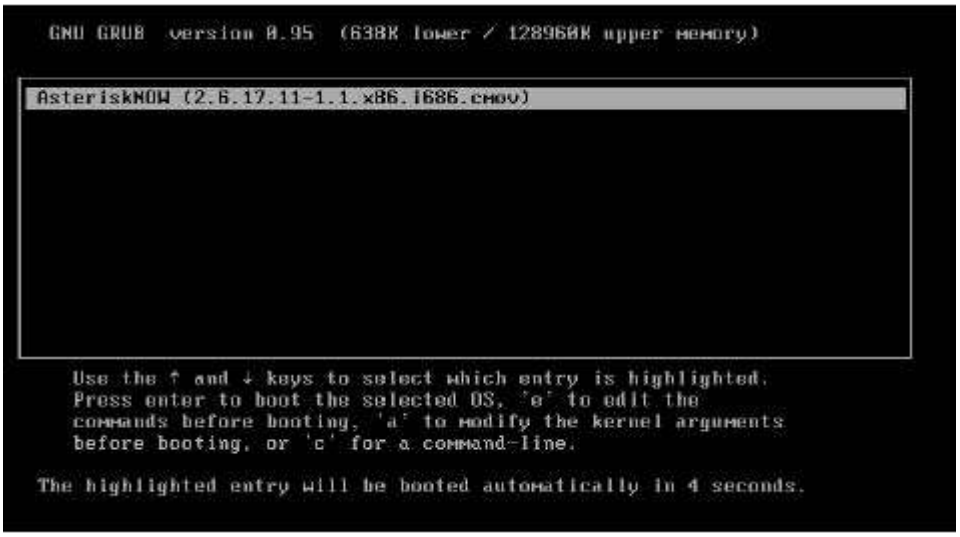
Luego comienza el proceso de instalación, que nos saldrán las siguientes pantallas.



Una vez finalizada la instalación, nos solicitara el reinicio

Primer arranque del Asterisk Now

Una vez finalizada la instalación, se ha reiniciado el PC, donde nos mostrará una pantalla que nos solicitara el núcleo de arranque. En un principio solo habrá uno.



La pantalla siguiente en el primer arranque de Asterisk Now, nos indica que existe un usuario llamado admin., y que su contraseña la hemos introducido durante el proceso de instalación.

Por último, el PC se quedara con la consola de Asterisk Now. Donde si deseamos podemos actualizar el sistema. El proceso de actualización será de varios minutos.

Administración del Asterisk a través de un navegador

Para ello, debemos tener un ordenador, con un navegador Web, donde introducimos la IP del servidor Asterisk. Donde cada vez, se nos solicitara si deseamos obtener un certificado para conectarnos. Esto provoca que todo lo que se transmita entre los dos PC sea de forma encriptada.

Lo siguiente que nos solicita es que introduzcamos el usuario ADMIN con su correspondiente contraseña.

La primera vez que ingresemos en el sistema Asterisk, se abrirá un asistente, que consisten en siete puntos. Donde se configuran los parámetros del funcionamiento.

Asignación de la contraseña al usuario Root

Para realizar la configuración a través de la edición de los ficheros de configuración, en algunas ocasiones, necesitaremos ser el usuario Root. Para ello, en la pantalla inicial, en la parte superior izquierda. Esta la opción de System Configuration.

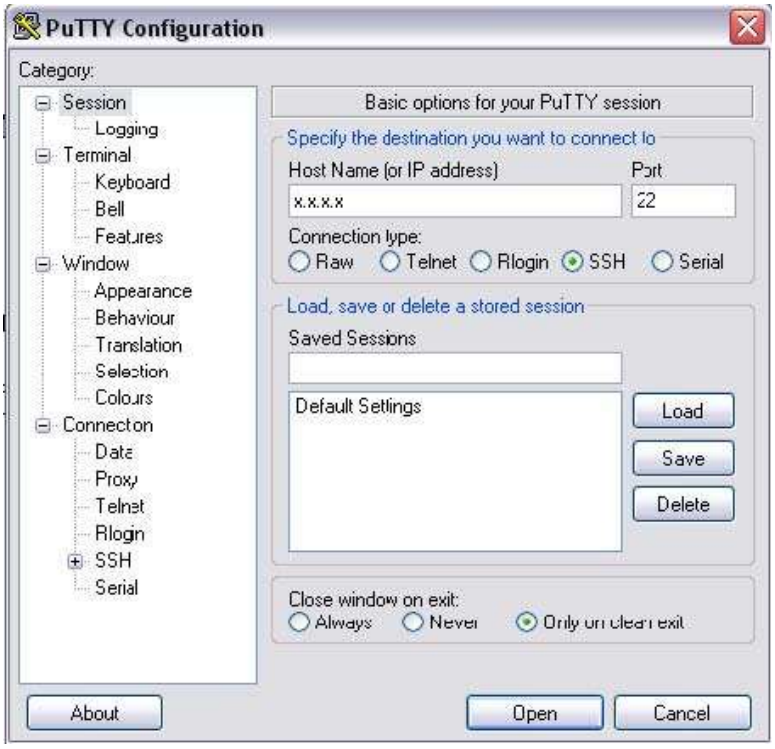
Donde nos solicitara que debemos introducir el usuario admin con su correspondiente contraseña.

Habrá un menú en la parte izquierda de la nueva pantalla que nos presenta, el menú Configuration, y dentro de él, un submenú Root password. En la cual podemos asignar una contraseña a nuestro usuario Root.

Además se puede configurar otros elementos sobre nuestro sistema.

Conexión a nuestro servidor

Para ello debemos conectarnos a nuestro servidor, se puede utilizar un programa llamado Putty. Donde el tipo de conexión debe ser SSH y donde pone Host Name o Ip Address, debemos introducir la IP del servidor.



Se abrirá una consola, donde solicitara un usuario para hacer login. Donde ingresaremos el usuario admin con su correspondiente contraseña. Si deseáramos para a usuario Root, debemos introducir el comando "su" e introducir la contraseña de Root.

Los ficheros de configuración de Asterisk se encuentran en la ruta /etc/asterisk

Configuración de SIP.CONF

En este fichero se definirán los usuarios, con sus correspondientes extensiones, numero a marcar para realizar una llamada.

Para realizar un comentario se deberá anteponer en la línea un “;”.

; USUARIO EJEMPLO

Para definir la extensión, de deberá poner entre corchetes.

[Número de extensión]

Definimos el tipo de extensión. Esta "User" se usa para autenticar llamadas entrantes, "peer" para llamadas salientes y "friend" para ambas

type=friend

Definimos la contraseña que tiene la extensión

secret=contraseña

Para definir que el tiempo de latencia no sea mayor que 2 seg.

qualify=yes

Si el dispositivo utiliza Nat

nat=no

El modo que se transmite los tonos

dtmfmode=info

Permitir al usuario conectarse de diferentes PC

host=dynamic

No permite conexión directa entre dos usuarios, siempre pasara por Asterisk

canreinvite=no

Nombre del contexto definido en extensions.conf

context=nombre

Correo de voicemail definido

mailbox=correo

Define un grupo de llamadas

callgroup=1

Define el grupo de llamadas válidas para una aplicación pickup

pickupgroup=1

Configuración del EXTENSIONS.CONF

En este fichero se define el contexto de las extensiones que hemos definido en SIP.CONF. Además, de indicar las acciones que se van a producir cuando le llame a una extensión.
Ahora vamos a ver una configuración para entender el funcionamiento.

En este ejemplo se van a definir tres contextos.
[pstn-in]; llamadas entrantes de línea telefónica
[outgoing_calls]; llamadas salientes de línea telefónica
[innova]; llamadas internas de la empresa Primero vamos a definir el contexto de llamadas entrantes. La definición para que pstn-in sea el contexto de llamadas entrantes será definida más adelante. Nombre del contexto de las llamadas entrantes
[pstn-in]

Pone a disposición las extensiones internas
include => dominio
Segundo vamos a definir el contexto de llamadas salientes. Donde la definición del contexto lo veremos más adelante.
Nombre del contexto de las llamadas salientes
[outgoing_calls]
Permite llamadas nacionales a fijos de Telefónica
exten => _9XXXXXXXX,1,Dial(Zap/1/${EXTEN})

Permite llamadas a móviles nacionales
exten => _6XXXXXXXX,1,Dial(Zap/1/${EXTEN})

Para él envió de fax, el funcionamiento será explicado más adelante
Exten => 200, 1, Dial (IAX2/ttyIAX/${EXTEN})
Para colgar la llamada
Exten => t, 1, Hangup ()

Tercero vamos a definir el contexto de llamadas internas. Aquí es importante poner el mismo nombre que el parámetro context del fichero SIP.CONF.
El siguiente ejemplo sirve para capturar las llamadas externas
Nombre del contexto
[Dominio]

Aquí se enumeran por orden de sucesión. Donde lo primero es preguntar
Exten => s, 1, Answer

Lo segundo que la espera sea de cero segundos
Exten => s, 2, Wait, 0

Lo tercero que llame a la extensión 7000 durante 15 segundos. Donde Tur, es para darle permiso de transferir llamadas y para que suene una música mientras se espera en la llamada
Exten => s, 3, Dial (SIP/7000, 15, Ttr)

Si la anterior extensión no ha cogido el teléfono, se llamara durante 30 segundos a la extensión 7010
Exten => s, 4, Dial (SIP/7010, 30, Ttr)

Si las dos extensiones anteriores no cogen el teléfono, saltara en buzón de voz de la extensión 7000
Exten => s,5,VoiceMail(7000@innova)

Se colgara la llamada
Exten => s, 6, Hangup
En el siguiente ejemplo, son las acciones que se producen cuando se realiza una llamada a una extensión interna

Si la llamada es a la extensión 7004, sonora durante 30 segundos el teléfono, donde el Atm, es para que el usuario pueda transferir las llamadas y para el que llame le suene una música.
Exten => 7000, 1, Dial (SIP/7004, 30, Ttm)
Si el usuario no coge el teléfono saltara el buzón de voz
Exten => 7000,2,VoiceMail(7004@dominio)
Una vez que la persona ha dejado el mensaje en el buzón de voz, oirá un mensaje de despedida
Exten => 7000, 3, PlayBack (vm-goodbye)

Se cerrara la llamada
Exten => 7000, 4, Hangup

Configuración de VOICEMAIL.CONF

Sirve para configurar el funcionamiento del buzón voz que tiene cada extensión. Cuando se defina el contexto, este deberá ser el mismo que hemos definido en el parámetro mailbox del fichero SIP.CONF.
El funcionamiento consiste que si en una llamada a una extensión no es cogida, pues salta el buzón de voz, donde sale una voz indicando que está en el buzón, que cuando suene la señal, podría dejar un mensaje de voz, el cual será enviado al correo que se haya definido.

Antes de empezar con la definición de los buzones de voz, vamos indicar una seria de parámetros interesantes.
Serveremail; es el e-mail que hace la notificación
attach=yes; el mensaje será enviado como dato adjunto
maxmessage=180; tamaño máximo del mensaje
minmessage=3; tamaño mínimo del mensaje
fromstring=Centralita; nombre de quien envía el e-mail

VM_NAME, VM_DUR, VM_MSGNUM, VM_MAILBOX, VM_CALLERID, VM_CIDNUM, VM_CIDNAME, VM_DATE; variables necesarias para componer el cuerpo del mensaje

emailsubject=Nuevo mensaje en su buzón de voz; especificación del asunto del mensaje
Emailbody=Estimado ${VM_NAME}:\n\n Alguien te ha dejado un correo de voz de ${VM_DUR} de duración en tu buzón ${VM_MAILBOX} de ${VM_CALLERID}.\n\n Deberías escucharlo en cuando tengas tiempo. Gracias\n\nCentralita; esto es un ejemplo del cuerpo del mensaje
Existe un contexto llamado [zonemessages], donde se definir la zona de los mensaje. Que en nuestro caso tenemos que definir que estamos en la zona de España, esto lo hacemos indicando la siguiente línea, spain=Europe/Madrid ‘Vmreceived' Q 'digits/at' R
Ahora vamos a definir el contexto de los mensajes de voz, que como he comentado, tiene ser el mismo que el definido en sip.conf en el parámetro mailbox
Nombre del contexto
[dominio]
Definición de la extension, de la contraseña, del nombre y del correo
7000 => 1234, Alumnouno, alumno.uno@dominio.com

Sección C.2

Instalación y configuración de SoftPhone

Para poder empezar a utilizar la centralita telefónica, necesitaremos teléfonos, para poder realizar llamadas. Se pueden utilizar teléfonos físicos o aplicaciones informáticas que hacen de teléfono.
La instalación es como cualquiera de las aplicaciones de Windows, donde con siguiente y siguiente, se realiza. Una vez instalado, debemos configurarlo para que

se conecte a nuestro Asterisk, para ello, debemos pulsar botón derecho sobre el teléfono y seleccionar la opción de “SIP Account Settings”

Donde nos saldrá una ventana, donde deberemos seleccionar la opción de Add. Lo que provocara que se abra otra ventana, donde deberemos poner la configuración. Donde un ejemplo es el siguiente.

Pasamos a detallar los valores de los campos:

Display Name: Ponemos nuestro nombre o un alias

User Name: Debemos poner la extensión (sip.conf parámetro entre corchetes) que nos ha asignado el administrador del Asterisk

Password: La contraseña (sip.conf el parámetro secret) asignada

Authorization user name: Debemos poner la extensión

Domain: La Ip del servidor que tiene instalado Asterisk

Si todo ha ido correcto, en la pantalla de Softone nos saldrá la siguiente imagen:

Si ha ido mal, saldrá el siguiente mensaje de error: Ahora ya dispondremos de una aplicación para poder realizar llamadas.

Anexo D

Sección D.1

Encuesta

ENCUESTA A DIRECTORES Y USUARIOS DEL SERVICIO Y LA RED

PREGUNTA	SI	NO
¿Ha tenido en cuenta la posibilidad de perder información, que se la roben, que no sea correcta?	90%	10%
¿Sabe Ud. si existen controles que detecten posibles fallos en la seguridad?	15%	85%
¿Conoce Ud. si existe un procedimiento de cifrado (seguridad) de las comunicaciones?	5%	95%
¿Existen reglas que regulen la transmisión de voz en sus enlaces?	10%	90%
¿Conoce si existen reglas que brinden seguridad en la transmisión de archivos (Datos) en sus enlaces?	10%	90%
¿Sabe si se utiliza algún medio para priorizar el tráfico de las aplicaciones de voz?	10%	90%
¿La transmisión y seguridad en sus enlaces para la transmisión de datos es eficiente?	50%	50%
¿La transmisión y seguridad de sus datos es segura?	20%	80%
¿La transferencia y seguridad de datos en los enlaces de comunicación es eficiente y confiable?	15%	85%
¿Ha tenido problemas en la transmisión de aplicaciones de voz cuando se satura el canal de comunicación?	5%	95%
¿Tienen un mecanismo de transporte los datos?	5%	95%

Sección D.2

Encuesta

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

ENCUESTA A ADMINISTRADORES DE REDES Y LABORATORISTAS

Lugar de aplicación de Encuesta: _____

Objetivo de la Encuesta.- Determinar la incidencia de los protocolos en la seguridad de la red al transmitir los datos

Sus respuestas le permitirán al investigador

-Desarrollar un trabajo real y efectivo.

- Agradecemos su colaboración

PREGUNTA	SI	NO
¿Existe políticas, normas y protocolos que regulen y aseguren la transmisión de los datos?	0%	100%
¿Qué tipo de protocolos se encuentran instalados en su red?	Por defecto Por defecto	
¿Cuáles de estos son utilizados en la Transmisión de VoIP?	Ninguno Ninguno	
¿Qué tipos de códecs son utilizados en conjunto con los protocolos, para mejorar la calidad y su seguridad?	Ninguno Ninguno	
¿Sabe de este tipo de transmisiones de VoIP sobre la red de la facultad?	75%	25%
¿Con que frecuencia es analizada la seguridad de transmisión de datos en la red de la facultad?	Casi Nunca	
¿Se ha analizado la posibilidad de que este tipo de comunicación (VoIP) sature el canal de comunicación?	95%	5%
¿Los protocolos implementados ayudan de manera eficiente en la transmisión de los datos?	5%	95%

¿La comunicación entre emisor y receptor es óptima en todo momento?	20%	80%
¿El modo de acceso al medio que utilizan los protocolos es el más recomendado?	5%	95%
¿Existe un procedimiento de cifrado de las comunicaciones?	5%	95%
¿Considera Usted que los protocolos utilizados en su red son los más eficientes?	5%	95%
¿Piensa Usted que los protocolos utilizados en su red son los más óptimos?	20%	80%
¿Considera Usted que los protocolos utilizados en su red tienen todo lo que necesitan para garantizar la seguridad en la red?	5%	95%

Anexo E

GUÍA DE INSTALACIÓN Y UTILIZACIÓN DE WIRESHARK

ETHEREAL es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. En el argo IT se denominan analizadores de protocolos de red, analizadores de paquetes, *packet sniffer* o *sniffer*. Ethereal permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Ethereal.

A partir del año 2006 Ethereal es conocido como **WireShark**[1] y hoy en día está categorizado como uno de los TOP 10 como *sniffer* junto a Nessus y Snort ocupando el segundo lugar entre estos.

Algunas de las características de WireShark son las siguientes:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

[1] A partir de esta nota nos referiremos a Ethereal como WireShark.

Es importante tener presente que WireShark no es un IDS (*Instrusion Detection System*) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Si embargo, permite a los profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red.

Instalación de WireShark

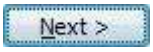
El instalador y los archivos binarios de Ethereal pueden ser descargados en http://www.ethereal.com/download.html y sus últimas versiones como se menciono anteriormente en http://www.wireshark.org/download.html. Adicional a esto en http://wiki.ethereal.com y http://wiki.wireshark.org podrás obtener una amplia cantidad de información relacionada con la aplicación, listas de correo tanto para usuarios finales como desarrolladores.

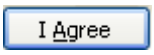
WireShark soporta múltiples plataforma entre ellas UNIX, LINUX y Windows, a continuación se describe la instalación para cada uno de estos sistemas operativos.

Instalación Windows

1. Una vez que se obtiene el instalador desde http://www.wireshark.org/download.html se ejecuta el archivo wireshark-setup-1.0.0.exe (en este caso la versión es 1.0.0) para iniciar la instalación. Es importante mencionar que las librerías necesarias como WinPcap están incluidas en el instalador.

Se muestra la siguiente pantalla del asistente:

2. Presionando el botón 

se despliega la especificación de la licencia y al presionar el botón 

se despliega la siguiente ventana para seleccionar los componentes que se desean instalar.

Para esta instalación se seleccionarán los siguientes:

- Wireshark, GUI del analizador de protocolos.
- TShark, línea de comando del analizador de protocolos. Plugins/Extensions, especificar plugins y extensiones para TShark y Wireshark en este punto deberá seleccionar todos los ítems listados.
- Tool, ofrece herramientas adicionales aplicar a los archivos que contienen los paquetes para su análisis seleccionar todas las ofrecidas durante la instalación.

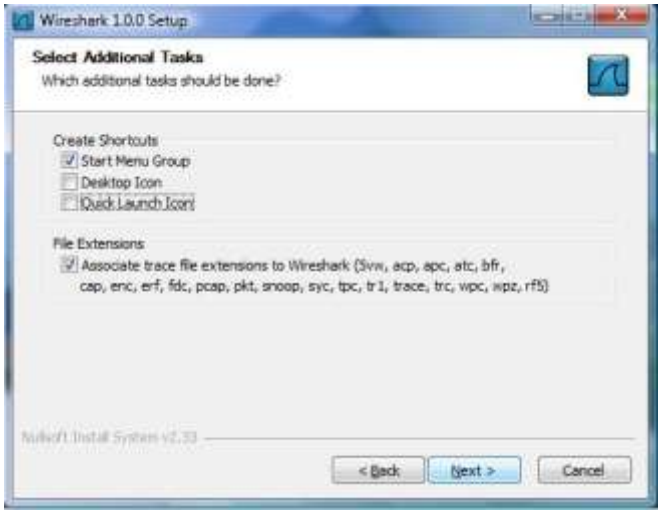
Editcap, para manipular los archivos.

Text2Pcap, convierte un archivo ASCII en formato libpcap.

Mergecap, permite obtener un archivo desde la combinación de 2 o más archivos de paquetes capturados.

Capinfos, es un programa que proporciona información de los paquetes capturados.

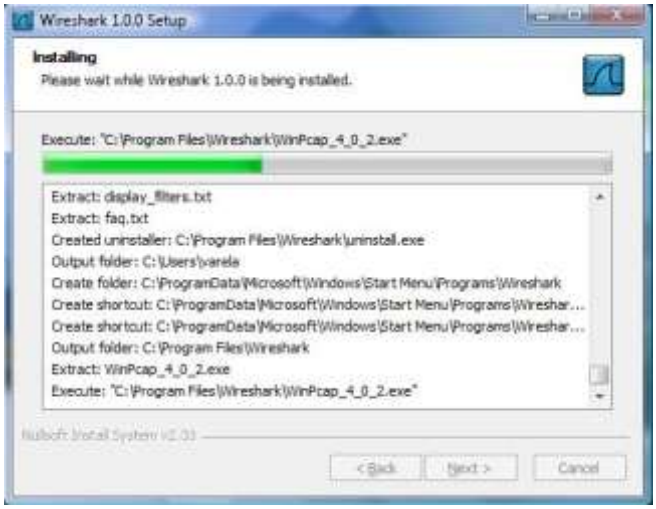
3. La siguiente pantalla permite seleccionar si se desea crear un acceso directo a la aplicación en el escritorio, crear un menú de inicio y visualizar el icono en la barra de tareas. Adicionalmente se tiene la posibilidad de permitir, que los archivos generados por otros analizadores de tráfico puedan ser visualizados con Wireshark (opción que debemos seleccionar).



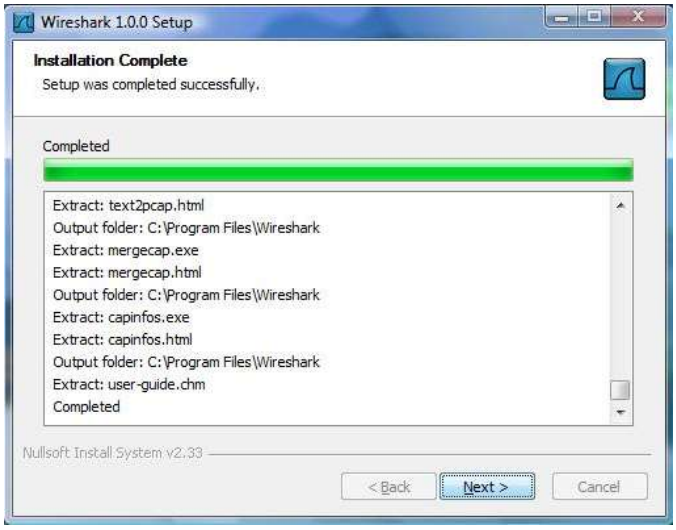
4. A continuación se deberá seleccionar el directorio donde se instalará la aplicación, en este punto se acepta el indicado por defecto en el instalador.

El instalador de WireShark contiene una versión de WinPcap que ofrece la opción de agregar un servicio para que usuarios que no tiene privilegios de administrador pueda capturar paquetes. En este punto se seleccionan ambos ítems.

Se presiona el botón Install para iniciar el proceso de instalación.



5. Como se mencionó anteriormente el instalador de WireShark para Windows permite hacer la instalación de las librerías, plugins, servicios, etc. Particularmente para el caso de WinPcap se interrumpe la instalación en el punto que muestra la pantalla arriba e inicia el asistente para la instalación de WinPcap. Se debe seleccionar Next > hasta finalizar la instalación.



La siguiente pantalla indica que la instalación ha finalizado exitosamente.

Para la actualización de WireShark se debe realizar el proceso descrito anteriormente. Se descarga la nueva versión y se ejecuta el instalador, una buena manera de estar actualizados en el mundo de Wireshark es a través de las lista de correo ofrecidas.

Interfaz de Usuario

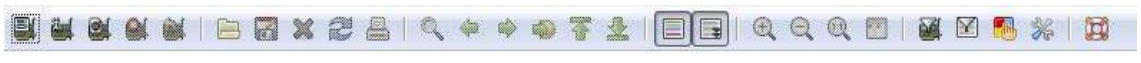
Existen dos maneras de iniciar la aplicación una es desde la línea de comando (*shell*) y otra desde el entorno gráfico. Cuando se inicia desde la línea de comando se tiene la posibilidad de especificar opciones adicionales que depende de las funciones que se quieran aprovechar.

La interfaz principal de WireShark cuenta con varias secciones:

- El Menú principal es utilizado para iniciar las acciones y/o funciones de la aplicación.

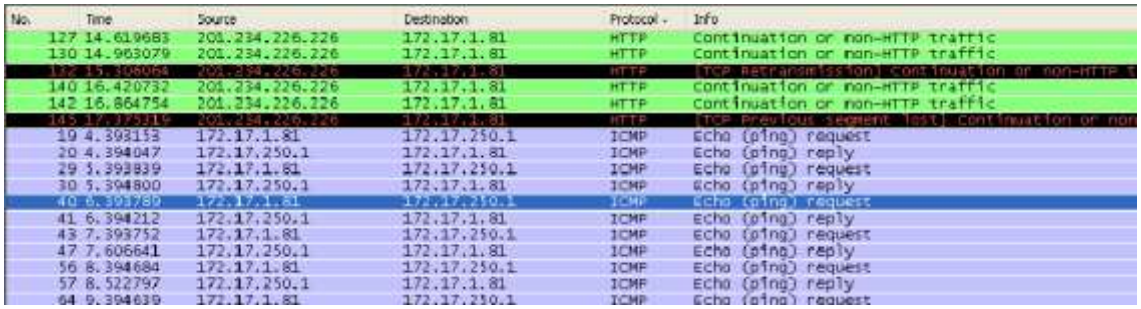
File, similar a otras aplicaciones GUI este contiene los ítems para manipular archivos y para cerrar la aplicación Wireshark.
Edit, este menú contiene ítems aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.
View, permite configurar el despliegue de la data capturada.
Go, contiene ítems que permiten el desplazamiento entre los paquetes.
Capture, para iniciar y detener la captura de paquetes.
Analyze, contiene ítems que permite manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.
Statistics, contiene ítems que permiten definir u obtener las estadísticas de la data capturada.
Help, menú de ayuda.

- Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.



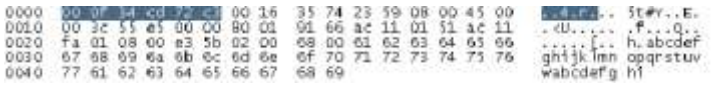
- Barra de herramientas para filtros, aquí se especifica el filtro que se desea aplicar a los paquetes que están siendo capturados.

- Panel de paquetes capturados, en este panel se despliega la lista de paquetes capturados. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.



- Panel para detalles del paquete, aquí se despliega información detallada del paquete seleccionado en el panel de paquetes.

- Panel de paquetes capturados en bytes, despliega en bytes la información contenida en el campo seleccionado desde el panel de detalles del paquete seleccionado en el panel de paquetes.



- La barra de estado, muestra información acerca del estado actual del programa y de la data capturada.

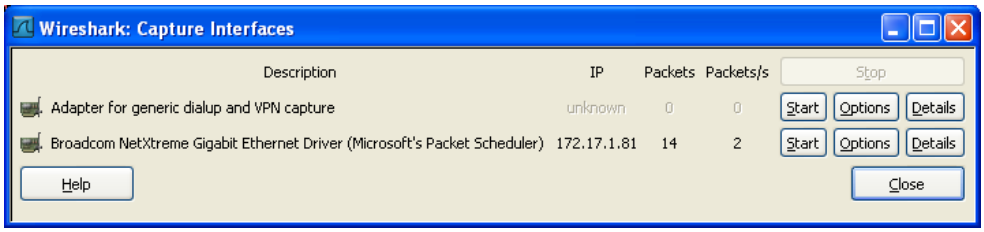
La interfaz de usuario puede ser cambiada desde el menú principal en la opción de *Preferences* en el menú *Edit*, según sea las necesidades.

Captura de Paquetes

Una de las principales funciones de WireShark es capturar paquetes con la finalidad de que los administradores y/o ingenieros de redes puedan hacer uso de estos realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos es ser administrador y/o contar con estos privilegios y es necesario identificar exactamente la interfaz que se quiere analizar.

WireShark cuenta con cuatro maneras para iniciar la captura de los paquetes:

1. Haciendo doble clic en  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.



Tres botones se visualizan por cada interfaz

- Start, para iniciar
- Options, para configurar
- Details, proporciona información adicional de la interfaz como su descripción, estadísticas, etc.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana donde se muestra opciones de configuración para la interfaz.

3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

4. Otra manera de iniciar la captura de paquetes es desde la línea de comandos ejecutando lo siguiente:

```
wireshark –i eth0 -k
```

Donde eth0 corresponde a la interfaz por la cual se desea iniciar la captura de paquetes.

Detener/Reiniciar la captura de paquetes

Para detener la captura de paquetes podemos aplicar una de las siguientes opciones:

- Haciendo uso del icono  desde el menú *Capture* o desde la barra de herramientas.
- Haciendo uso de ctrl+E.
- La captura de paquetes puede ser detenida automáticamente, si una de las condiciones de parada definidas en las opciones de la interfaz se cumple, por ejemplo: si se excede cierta cantidad de paquetes.

Para reiniciar el proceso de captura de paquetes se debe seleccionar el icono  en la barra de herramientas o en desde el menú *Capture*.

Filtrado de paquetes

Wireshark hace uso de libpcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (*and/or*) con la opción de ser negada por el operador *not*.

```
[not] Expresión [ and|or [not] expresión…]
```

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP x.y.z.w y a.b.c.d

```
ip.addr==172.17.250.1 and ip.addr==172.17.1.81
```

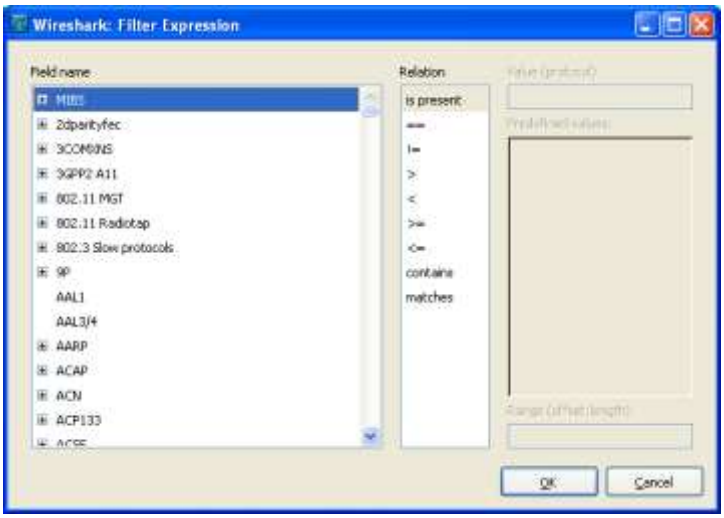
En el site http://wiki.wireshark.org/CaptureFilters podrá obtener una serie de filtros que son usualmente aplicados por los administradores de red.

Expresiones de filtrado

WireShark proporciona una poderosa herramienta para construir filtros más complejos. Permite comprar valores así como también combinar expresiones dentro de otra expresión.

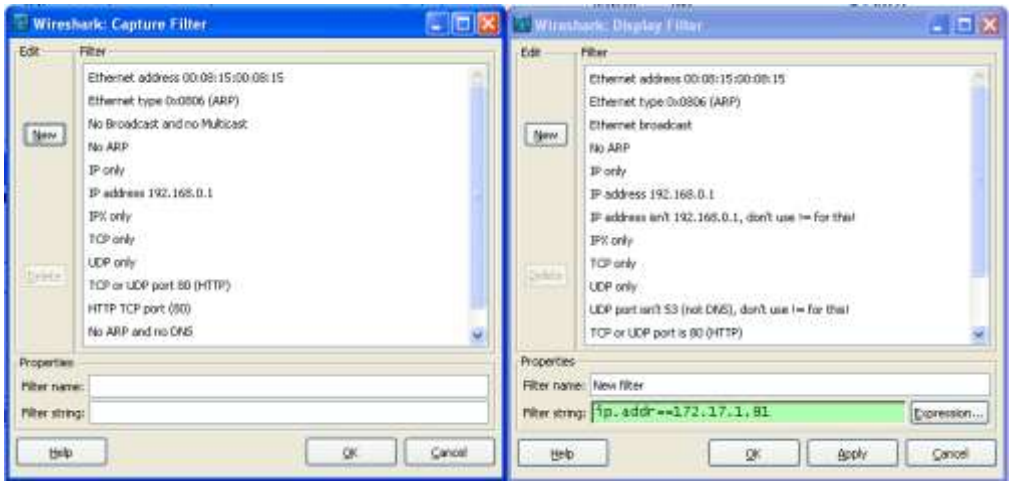
En el site http://wiki.wireshark.org/DisplayFilters podrá obtener una serie de expresiones que son usualmente aplicados por los administradores de red.

Cuando es bien conocido el campo por el cual se requiere hacer el filtrado es recomendable hacer uso de *Filter Expresion* desde la barra de herramientas para filtros presionando *Expresion…* facilitando la construcción de la expresión o fórmula seleccionando el campo (*field name*), el operador (Relation) y el valor contra el cual se quiere comparar.



Es muy común que ciertos filtros y/o expresiones requieran ser utilizado en un futuro, para esto Wireshark permite definir los filtros y/o expresiones y guardarlas.

Para guardar o abrir un filtro existente (previamente creado y guardado) se debe seleccionar *Display Filter* en el menú *Analize* o *Capture Filter* que se encuentra en el menú *Capture.*

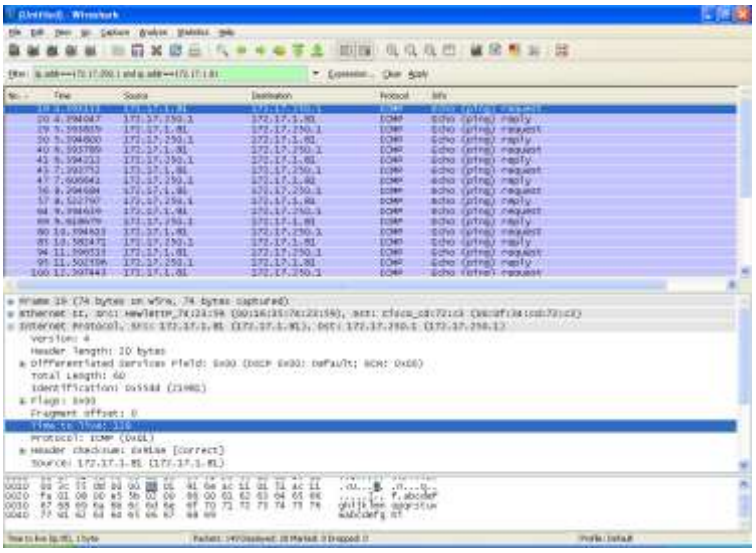


Para definir un filtro se debe presionar el botón New se indica el nombre del filtro y la expresión y presionar OK para salvar los cambios.

Manipulando las paquetes capturados (análisis)

Una vez que se tienen capturados los paquetes estos son listados en el panel de paquetes capturados, al seleccionar uno de estos se despliega el contenido del paquete en el resto de los paneles que son panel de detalles de paquetes y panel en bytes.

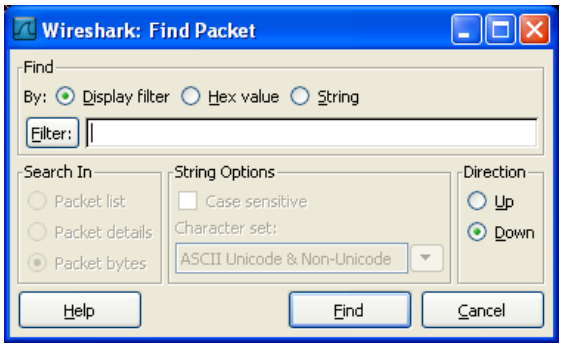
Expandiendo cualquiera parte del árbol presentado en el panel de detalle del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes. En la siguiente imagen se identifica en campo TTL del la cabecera del IP.



Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura esto se logra, seleccionando la opción *Update list packets in real time* desde menú *Edit->Preferentes->Capture*. Adicionalmente, Wireshark permite visualizar el contenido de un paquete seleccionado en el panel de paquetes capturados en una ventana individualmente seleccionando la opción Show Packet in new Windows en menú principal *View*. Esto permite comparar con más facilidad dos o más paquetes.

Función de búsqueda de paquetes

Cuando iniciamos la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y/o expresiones definidas, Wireshark permite realizar búsqueda(s) de paquete(s) que tienen cierta característica. Para esto se debe seleccionar la opción *Find Packet* en el menú *Edit* se despliega la siguiente ventana.



Se rellena el campo *Filter* con el criterio de búsqueda que se desea y el resto de los campos seguidamente se presiona el botón de búsqueda.

Otra opción es realizar la búsqueda del paquete anterior y próximo al que esta seleccionado en el panel de paquetes esto se aplica desde el menú de *Edit* las opciones *Find Next* y *Find Previous*.

Visualizando estadísticas

WireShark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú *Statistics* que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo. Podemos distinguir entre cada una de las anteriores:

Estadísticas Generales

- Summary, la cantidad de paquetes capturados.
- Protocol Hierarchy, presenta las estadísticas para cada protocolo de forma jerárquica.
- Conversations, un caso particular es el tráfico entre una IP origen y una IP destino.
- Endpoints, muestra las estadísticas de los paquetes hacia y desde una dirección IP.
- IO Graphs, muestra las estadísticas en grafos.

Estadísticas específicas de los protocolos

- Service Response Time entre la solicitud (*request*) y la entrega *(response*) de algún protocolo existente.
- Entre otras.

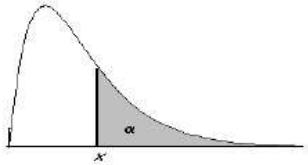
Es importante tener presente que los números arrojados por estas estadísticas solo tendrán sentido si se tiene un conocimiento previo el protocolo de lo contrario serán un poco compleja de comprender.

Anexo F

Tabla de distribucion de (X2)

Tabla de la distribución chi-cuadrado.

La tabla contiene los valores x tales que $p\left[\chi_n^2 \geq x\right] = \alpha$ en función de los grados de libertad (n).



n	0,99	0,98	0,975	0,95	0,90	0,80	0,50	0,20	0,10	0,05	0,025	0,02	0,01	0,001
1	0,0002	0,0006	0,0010	0,0039	0,0158	0,0642	0,4549	1,6424	2,7055	3,8415	5,0239	5,4119	6,6349	10,8274
2	0,0201	0,0404	0,0506	0,1026	0,2107	0,4463	1,3863	3,2189	4,6052	5,9915	7,3778	7,8241	9,2104	13,8150
3	0,1148	0,1848	0,2158	0,3518	0,5844	1,0052	2,3660	4,6416	6,2514	7,8147	9,3484	9,8374	11,3449	16,2660
4	0,2971	0,4294	0,4844	0,7107	1,0636	1,6488	3,3567	5,9886	7,7794	9,4877	11,1433	11,6678	13,2767	18,4662
5	0,5543	0,7519	0,8312	1,1455	1,6103	2,3425	4,3515	7,2893	9,2363	11,0705	12,8325	13,3882	15,0863	20,5147
6	0,8721	1,1344	1,2373	1,6354	2,2041	3,0701	5,3481	8,5581	10,6446	12,5916	14,4494	15,0332	16,8119	22,4575
7	1,2390	1,5643	1,6899	2,1673	2,8331	3,8223	6,3458	9,8032	12,0170	14,0671	16,0128	16,6224	18,4753	24,3213
8	1,6465	2,0325	2,1797	2,7326	3,4895	4,5936	7,3441	11,0301	13,3616	15,5073	17,5345	18,1682	20,0902	26,1239
9	2,0879	2,5324	2,7004	3,3251	4,1682	5,3801	8,3428	12,2421	14,6837	16,9190	19,0228	19,6790	21,6660	27,8767
10	2,5582	3,0591	3,2470	3,9403	4,8652	6,1791	9,3418	13,4420	15,9872	18,3070	20,4832	21,1608	23,2093	29,5879
11	3,0535	3,6087	3,8157	4,5748	5,5778	6,9887	10,3410	14,6314	17,2750	19,6752	21,9200	22,6179	24,7250	31,2635
12	3,5706	4,1783	4,4038	5,2260	6,3038	7,8073	11,3403	15,8120	18,5493	21,0261	23,3367	24,0539	26,2170	32,9092
13	4,1069	4,7654	5,0087	5,8919	7,0415	8,6339	12,3398	16,9848	19,8119	22,3620	24,7356	25,4715	27,6882	34,5274
14	4,6604	5,3682	5,6287	6,5706	7,7895	9,4673	13,3393	18,1508	21,0641	23,6848	26,1189	26,8727	29,1412	36,1239
15	5,2294	5,9849	6,2621	7,2609	8,5468	10,3070	14,3389	19,3107	22,3071	24,9958	27,4884	28,2595	30,5780	37,6978
16	5,8122	6,6142	6,9077	7,9616	9,3122	11,1521	15,3385	20,4651	23,5418	26,2962	28,8453	29,6332	31,9999	39,2518
17	6,4077	7,2550	7,5642	8,6718	10,0852	12,0023	16,3382	21,6146	24,7690	27,5871	30,1910	30,9950	33,4087	40,7911
18	7,0149	7,9062	8,2307	9,3904	10,8649	12,8570	17,3379	22,7595	25,9894	28,8693	31,5264	32,3462	34,8052	42,3119
19	7,6327	8,5670	8,9065	10,1170	11,6509	13,7158	18,3376	23,9004	27,2036	30,1435	32,8523	33,6874	36,1908	43,8194
20	8,2604	9,2367	9,5908	10,8508	12,4426	14,5784	19,3374	25,0375	28,4120	31,4104	34,1696	35,0196	37,5663	45,3142
21	8,8972	9,9145	10,2829	11,5913	13,2396	15,4446	20,3372	26,1711	29,6151	32,6706	35,4789	36,3434	38,9322	46,7963
22	9,5425	10,6000	10,9823	12,3380	14,0415	16,3140	21,3370	27,3015	30,8133	33,9245	36,7807	37,6595	40,2894	48,2676
23	10,1957	11,2926	11,6885	13,0905	14,8480	17,1865	22,3369	28,4288	32,0069	35,1725	38,0756	38,9683	41,6383	49,7276
24	10,8563	11,9918	12,4011	13,8484	15,6587	18,0618	23,3367	29,5533	33,1962	36,4150	39,3641	40,2703	42,9798	51,1790
25	11,5240	12,6973	13,1197	14,6114	16,4734	18,9397	24,3366	30,6752	34,3816	37,6525	40,6465	41,5660	44,3140	52,6187