UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

SEMINARIO DE GRADUACIÓN "SISTEMAS Y REDES DE COMUNICACIÓN INALAMBRICA"

Tema:

"CONEXIÓN VPN PARA ACCESO REMOTO ENTRE EL EDIFICIO DEL H. GOBIERNO PROVINCIAL DE TUNGURAHUA Y SUS BODEGAS UBICADAS EN EL SECTOR DE CATIGLATA"

Trabajo de Graduación Modalidad: Seminario de Graduación, presentado previo a la obtención del título de Ingeniero en Electrónica y Comunicaciones

AUTOR: Portero Nuela Daniel Fabricio

TUTOR: Ing. M. Sc. Elsa Pilar Urrutia Urrutia

Ambato - Ecuador

Octubre 2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema:
"CONEXIÓN VPN PARA ACCESO REMOTO ENTRE EL EDIFICIO DEL H. GOBIERNO PROVINCIAL DE TUNGURAHUA Y SUS BODEGAS UBICADAS EN EL SECTOR DE CATIGLATA", del señor Daniel Fabricio Portero Nuela, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato.

Ambato Octubre 17, 2012

EL TUTOR

Ing. M. Sc. Elsa Pilar Urrutia Urrutia

AUTORÍA

El presente trabajo de investigación titulado: "CONEXIÓN VPN PARA ACCESO REMOTO ENTRE EL EDIFICIO DEL H. GOBIERNO PROVINCIAL DE TUNGURAHUA Y SUS BODEGAS UBICADAS EN EL SECTOR DE CATIGLATA". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Octubre 17, 2012

Daniel Fabricio Portero Nuela

CI: 180437132-4

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Mario Geovanni García Carrillo e Ing. Marco Antonio Jurado Lozada, revisó y aprobó el Informe Final del trabajo de graduación titulado Conexión VPN para acceso remoto entre el edificio del H. Gobierno Provincial de Tungurahua y sus bodegas ubicadas en el sector de Catiglata, presentado por el señor Daniel Fabricio Portero Nuela de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato Octubre 17, 2012

Ing. M. Sc. Oswaldo Eduardo Paredes Ochoa
PRESIDENTE DEL TRIBUNAL

Ing. M. Sc Mario Geovanni García Carrillo
DOCENTE CALIFICADOR

Ing. M. Sc. Marco Antonio Jurado Lozada
DOCENTE CALIFICADOR

DEDICATORIA:

A Dios, porque siempre me ha bendecido y sobre todo en la realización de este proyecto.

A mis padres, Fausto y Beatriz que con su apoyo incondicional me han enseñado que nunca hay que darse por vencido.

A mis hermanos que de una u otra manera me dieron su apoyo, tanto económico como moral.

A mis amigos con los que compartí muchas cosas en el transcurso de la universidad, aquellos que supieron darme una palabra de apoyo.

Daniel F. Portero N.

AGRADECIMIENTO:

A la Universidad Técnica de Ambato y en especial a la Facultad de Ingeniería en Sistemas Electrónica e Industrial por acogerme y permitir cumplir mis metas.

Al departamento de sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA por brindarme apoyo en el desarrollo del proyecto.

A mis padres por brindarme su confianza y apoyo ya que sin ellos no lo hubiera logrado.

Daniel F. Portero N.

INDICE

INDICE DE GRÁFICOS

INDICE DE TABLAS

RESUMEN EJECUTIVO

El presente proyecto tiene como objetivo Principal brindar comunicación en lo referente a servicios de Voz y Datos entre las Bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y su departamento de sistemas, utilizando una Red Privada Virtual (VPN) que permita una conexión segura través de Internet.

En el capítulo I se especifica el planteamiento del problema que se define como, el deficiente sistema de comunicación entre las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y su matriz, es ahí que surge la necesidad de establecer Conexión VPN para la comunicación entre estos dos lugares.

El capítulo II se refiere al Marco Teórico, encontramos la fundamentación legal en donde se habla de las leyes que abarcan al proyecto investigado, la explicación de las variables correspondientes a las Categorías Fundamentales, a través de la investigación documental bibliográfica.

La hipótesis planteada fue: La subutilización de la red genera un deficiente sistema de comunicación entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas. Lo que significa que el mal uso de la red perjudica al HGPT, ya que al no abastecer las necesidades de conexión la comunicación es deficiente, de esta hipótesis se desprenden las variables dependientes e independientes, con su respectiva Operacionalización.

El capítulo III habla del enfoque y el tipo de investigación que se realizo, tuvo una modalidad cuali-cuantitativa ya que estaba orientado a identificar y a entender las causas del problema; esta investigación ostentó los tipos de investigación exploratorio y descriptivo ya que fue necesario tener un conocimiento suficiente del problema que se suscito en el HGPT.

El Capítulo IV contiene el análisis de resultados, con lo cual para lograr los objetivos propuestos se realizó un trabajo de Campo, con el fin de recolectar la información a través de la entrevista realizada al Administrador del departamento de sistemas del HGPT y la Observación elaborada con el fin de ver el estado de los equipos del HGPT, los datos obtenidos sirvieron para analizar e interpretar la situación actual en la que se encuentra el HGPT.

El capítulo V trata de las conclusiones y recomendaciones que se obtuvo al realizar la observación y la entrevista, con las cuales el HGPT al aceptar y ponerlas a la práctica, se convertirán en orientaciones eficientes que servirán como una herramienta útil para el mejoramiento de las comunicaciones en los diferentes departamentos del mismo.

El capítulo VI habla del desarrollo del proyecto, la cual es una conexión VPN mediante la cual se transmiten los servicios de voz y datos de una forma segura. Se realiza las pruebas apropiadas para comprobar el buen funcionamiento de la conexión, del envió de información y la transmisión de voz, dando así a notar que el proyecto puede ser implementado en cualquier empresa.

INTRODUCCIÓN

Actualmente el internet se esta desarrollando potencialmente, esto ha permitido el progreso de sistemas que permiten establecer comunicación de forma segura entre sucursales que pertenecen una misma entidad o estaciones remotas, este es el caso de una Conexión VPN (Red Privada Virtual).

Una Conexión VPN permite que la información viaje de un punto a otro de una manera segura, para lograr esto se crea las llaves y certificados que van ser el mayor respaldo de seguridad al establecer comunicación.

El presente proyecto se basa en realizar una conexión VPN mediante el protocolo SSL/TLS con la ayuda del Software OpenVPN en Ubuntu 12.04, con el objetivo de asegurar la información generada, y brindar servicio de voz y datos entre las bodegas del H.GOBIERNO PROVINCIAL DE TUNGURAHUA y su departamento de sistemas.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema

"Conexión VPN para acceso remoto entre el edificio del H. Gobierno Provincial de Tungurahua y sus bodegas ubicadas en el sector de Catiglata"

1.2 Planteamiento del problema

1.2.1 Contextualización

La tecnología VPN cada vez se va desarrollando a nivel mundial, ya que estas permiten la comunicación desde distintos lugares con nuestra información, o ya sea para la transmisión desde sitios de difícil acceso con un radio enlace, tanto así que se ha podido encontrar diferentes beneficios en las distintas configuraciones que tiene una VPN en diferentes empresas ya que estas permiten conexiones a sus clientes, empleados o proveedores.

Las VPNs son muy usadas hoy en día, ya que permiten el acceso seguro a las redes de la empresa, usando internet de manera rápida y eficiente. Ya que la comunicación es esencial, pero al efectuarse en grandes distancias el problema

que se presenta son los costos, debido a esto muchas instituciones públicas y privadas han optado por diseñar redes de acceso ya que necesitan intercambiar información con sus sucursales o sociedades

En nuestro país el desarrollo de las actividades personales, empresariales e institucionales, en fin las actividades de negocio dan la necesidad de proveerse de redes de acceso que les permitan la comunicación de una manera fácil y rápida, sobretodo de bajo costo es por eso que se ha querido tomar ventaja de las redes públicas de amplio alcance, como es el caso del internet, red que ha tomado popularidad en todo negocio y actividad diaria, sobre todo que ha impulsado una nueva forma de comunicación que es las redes privadas virtuales VPN.

En Tungurahua la transferencia de información se ha convertido en un elemento importante en las organizaciones, sobre todo en las empresas que se encuentran distribuidas a nivel nacional o a lo largo de la provincia los cuales necesitan tener acceso a sus bases de datos o que necesiten enviar información, frecuentemente algunas instituciones no cuentan con estas conexiones ya que resultan muy costosas sobre todo si se trata de largas distancias. Por tal razón la información llega con retardos y corre el riesgo de ser alterada en el camino.

En nuestro medio el internet no ha tenido un uso adecuado en lo relacionado a su desarrollo en redes de comunicación, algunas instituciones públicas o privadas no han aprovechado este servicio como un medio para comunicarse con sus sucursales, bodegas y/o empleados, este es el caso del H. GOBIERNO PROVINCIAL DE TUNGURAHUA, ya que esta entidad pública al reubicar sus bodegas no cuentan con un sistema que enlace estos dos puntos para la transmisión de información y servicios de voz y datos con lo cual se mejoraría tanto el control como la seguridad.

1.2.2 Árbol Del Problema

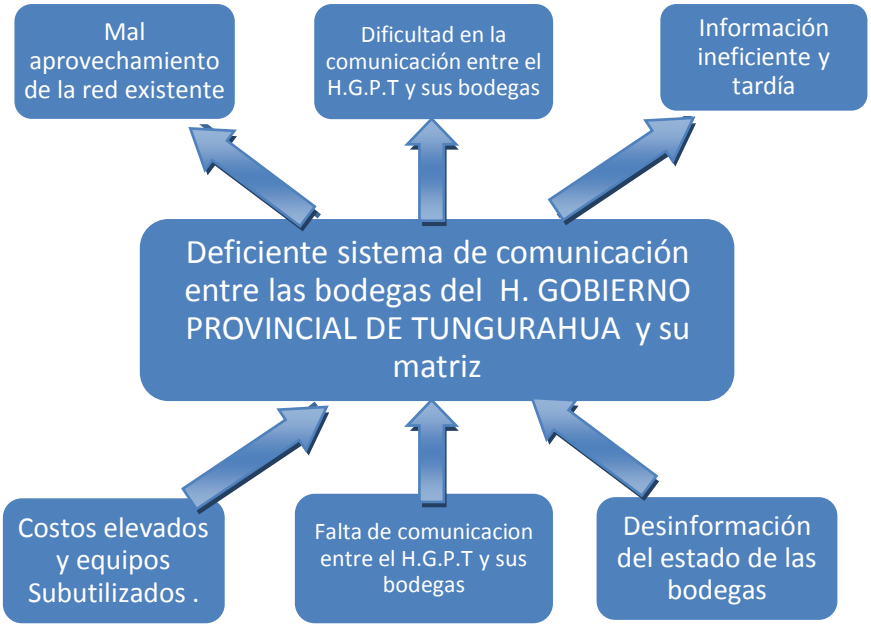


Gráfico Nº 1.1 Árbol del Problema

Elaborado por: El investigador

1.2.3 Análisis Crítico

A nivel mundial, se ha escrito mucho sobre las nuevas tecnologías de comunicación, las mismas que se han venido desarrollando e implementando desde su apogeo, sobre todo las comunicaciones que permiten a usuarios el acceso desde cualquier lugar en el que se encuentre a la información de sus compañías o pequeñas empresas tan solo con conectarse a internet, en Ambato se encuentra el GOBIERNO PROVINCIAL de TUNGURAHUA una entidad que cuenta con un sistema de comunicación que lo subutiliza, ya que a los equipos de comunicación utilizados no les dan un mantenimiento periódico, motivo por el cual algunos ya están en desuso y su reparación involucra grandes costos, es por eso que la red de las bodegas antiguas no puede ser utilizado en las bodegas de Catiglata.

La falta de un sistema de comunicación entre las bodegas y el edificio principal del H.G.P.T ha provocado dificultades en la comunicación como no poder enviar información, recibir los informes de estado de materiales, enviar alertas de seguridad, etc. En muchos casos la comunicación es nula.

Saber el estado en el que se encuentran las bodegas del H.G.P.T es muy importante para los funcionarios del departamento de sistemas, pero existe desinformación entre estas dos localidades, lo cual ha provocado que la información sea ineficiente y tardía, y exista desactualización de datos.

1.2.4 Prognosis

Las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA, al no tener un sistema de conexión VPN como una alternativa tecnológica de comunicación no podrán mantener una conexión segura y así tampoco podrá compartir recursos e información entre la bodega en sí y su edificio principal.

1.2.5 Formulación Del Problema

¿La subutilización de la red existente genera un deficiente sistema de comunicación entre el edificio del H. GOBIERNO PROVINCIAL DE TUNGURAHUA Y SUS BODEGAS en el sector de Catiglata?

1.2.6 Preguntas Directrices

- ¿Cuál es la situación actual de las comunicaciones entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas?

- ¿Cuáles son las características de una conexión VPN y de la Red que posee el H. GOBIERNO PROVICIAL DE TUNGURAHUA?

- ¿Qué tecnología es la más adecuada para garantizar la comunicación entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas ubicadas en el sector de Catiglata?

1.2.7 Delimitación Del Problema

CAMPO: Ingeniería Electrónica y Comunicaciones
ÁREA: Telecomunicaciones
ASPECTO: Sistema de comunicaciones VPN
DELIMITACIÓN ESPACIAL: El estudio de este proyecto se realizó en las instalaciones del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas que se encuentran en la ciudad de Ambato en el sector de Catiglata.
DELIMITACIÓN TEMPORAL: El presente proyecto de investigación tuvo una duración de 6 meses, a partir de que este fue aprobado por el Honorable Concejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 Justificación

Actualmente el aprovechamiento tecnológico ha sido muy extenso ya que día a día la ciencia y la tecnología avanzan rápidamente y sobre todo son bienes necesarios para las personas ya que facilitan el trabajo en diferentes campos tanto económicos, sociales, educativos, ocio y sobre todo en el campo empresarial es por eso que es muy necesario tener un sistema de comunicación para la transmisión de datos ya que hay empresas que cuentan con sucursales o bodegas que se encuentran ya sea cerca o en lugares distantes de su matriz principal.

Resulta de vital importancia el estudio de este proyecto ya que esta tecnología permitirá integrar servicios de voz y datos con lo cual tendremos optimización en los procesos y la seguridad a nivel general en las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA.

El estudio de la red privada virtual permite establecer una conexión para el transporte de la información, permitiendo que se enlace dos puntos del H. GOBIERNO PROVINCIAL DE TUNGURAHUA por medio del internet.

Los beneficios de este proyecto de investigación se verán reflejados en la optimización de los recursos, en la comunicación eficaz , en la seguridad tanto de las instalaciones como del material y el cumplimiento de objetivos operacionales, la institución podrá hacer los cambios en las áreas que sean pertinentes, los mismos que conducirán a incrementar la seguridad y la confiabilidad de la comunicación de la misma y por ende los beneficiados serán, las personas que se encuentran al frente de la dirección y los empleados de la institución.

La información se obtuvo en el lugar mismo de la investigación, por cuanto la gerencia facilito todo tipo de información y los recursos que fueron necesarios para la realización de este trabajo.

Finalmente esta investigación fue muy factible ya que se contó con los recursos técnicos y humanos, en este caso el apoyo del departamento de sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA que fue el apoyo primordial ya que facilito los datos necesarios de la investigación.

1.4 Objetivos

1.4.1 Objetivo general:

Analizar el uso de la red existente y su efecto en el deficiente sistema de comunicación entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas.

1.4.2 Objetivos específicos:

1) Realizar un estudio sobre el uso real de la red del edificio del H. GOBIERNO PROVINCIAL DE TUNGURAHUA.

2) Analizar el sistema de comunicación aplicado actualmente entre el edificio del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas.

3) Proponer una conexión VPN que permita mejorar el sistema de comunicación proporcionando la transmisión de información y servicios triple Play entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas ubicadas en el sector de Catiglata.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

En la facultad de INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL después de revisar los archivos de tesis existente se ha encontrado que hay tres trabajos similares o relacionados con esta investigación.

"VPN para facilitar la comunicación entre las oficinas centrales y las bodegas de la constructora LOPEZ CÍA LTDA", presentado por Paul Espinoza. (2010).

La conclusión de este proyecto es que para la constructora LOPEZ CÍA LTDA se logro crear redes virtuales privadas seguras y a muy bajo costo mediante OpenVPN.

"Red privada virtual (VPN) para la transmisión de servicios multimedia sobre IP entre la COOPERATIVA DE AHORRO Y CRÉDITO AMBATO LTDA. y sus sucursales", presentado por Roberto Noé Molina Salas (2011).

Se puede concluir que a través de este proyecto se puede transmitir cualquier tipo de información, pudiendo ser en este caso voz y datos, que beneficio a la Cooperativa de Ahorro Ambato Ltda.

"Estudio de factibilidad para la implantación de VPNs a través de Internet en la operadora de turismo "QUIMBAYA TOURS INTERNATIONAL HOLDING", presentado por Cecilia Díaz y Mónica García. (2005).

Se concluye que la tecnología VPN tiene grandes proyecciones de crecimiento e implantación en la operadora de turismo QUIMBAYA debido a que reduce costos, brinda mayor seguridad y no es necesario un proveedor de servicio, sino solamente un proveedor de enlace.

2.2 Fundamentación Legal

Esta tesis tiene como fundamentación legal, la Ley especial de Telecomunicaciones y sus reformas, asi como los organismos de control de las telecomunicaciones.

2.2.1 Organismos de Control de Telecomunicaciones

MINTEL: El Ministerio de Telecomunicaciones y de la Sociedad de la Información es el órgano rector del desarrollo de las Tecnologías de la Información y Comunicación en el Ecuador, que emite políticas, planes generales y realiza el seguimiento y evaluación de su implementación, coordinando acciones de asesoría y apoyo para garantizar el acceso igualitario a los servicios y promover su uso efectivo, eficiente y eficaz.

CONATEL: El Consejo Nacional de Telecomunicaciones es el ente que tiene la representación del Estado para administrar y regular las telecomunicaciones ante la unión internacional de telecomunicaciones (UIT).

SENATEL: La Secretaría Nacional De Telecomunicaciones es el organismo encargado de la ejecución de las políticas en telecomunicaciones en el país.

SUPERTEL: La Superintencia De Telecomunicaciones tiene como misión vigilar, auditar, intervenir y controlar técnicamente la prestación de los servicios de telecomunicaciones, radiodifusión, televisión y el uso del espectro.

2.2.2 H. Gobierno Provincial de Tungurahua

El Honorable Gobierno Provincial de Tungurahua es una entidad de poder público que ejerce el gobierno, la administración y representación política del estado en la jurisdicción provincial (ref. Arts. 224, 228 y 233 C.P.E.). Se rige por una ley orgánica (actual ley de régimen provincial, vigente desde el 10 de febrero de 1969 misma que será reformulada por el H. Consejo Nacional a iniciativa de CONCOPE). En ella su estructura de integración, deberes y atribuciones solo mediante ley puede atribuírseles cargos y deberes (ref. Art. 142, 230, y 141 de la C.P.E.).

Reseña Histórica

Don Oscar Efrén Reyes y Don Juan Francisco Montalvo en 1.928, al reseñar el génesis de la Provincia de Tungurahua en la vida republicana del país, en la monografía de la provincia escrita en ese año nos dicen:

"1860.- DE CANTON A PROVINCIA.- La Notoria importancia del Cantón de Ambato, como uno de los primeros pueblos de la República; la influencia de muchos de sus hijos en la vida nacional y sus gallardas actitudes ante las nobles causas, fueron al fin justipreciadas.

Para el año de 1860, ya no hay quienes discutan la necesidad de elevar a Provincia esta sección del país, y, antes bien todos coinciden en ella. Así le toca al Gobierno Provisional presidido por los señores Manuel Gómez de la Torre, José María Aviléz y Rafael Carvajal, expedir el correspondiente decreto, que lo transcribimos, por los detalles anexos que contiene respecto del número de los cantones que debían componer la nueva Provincia de Ambato".

Fue el 3 de julio de 1.860 que nuestra actual jurisdicción nació como provincia del estado ecuatoriano. Desde ahí, la indómita voluntad de sus habitantes la hizo crecer, la hizo próspera; en esta empresa ha sido capital la decisión de sus

instituciones y con ellas o en ellas la actitud constructiva de sus hombres y mujeres.

El H. Gobierno Provincial de Tungurahua, pese a su corta vida en el lapso de existencia de la provincia ha jugado un papel preponderante en el desarrollo de la jurisdicción; nuestra institución, la principal y de mayor jerarquía en la provincia se configura en 1.946 con sus actuales objetivos, estructura y roles que le confiriera la Constitución Política de ese entonces.

Bajo los principios de representatividad, corresponsabilidad y gobernabilidad trabajamos en el mejoramiento de las condiciones de vida, mejorar la calidad y la cantidad del agua, así como el incremento de fuentes de empleo e incremento de ingresos como objetivos comunes hacia el futuro.

Hemos conseguido orgullosamente logros como; Fondo de manejo de Páramos y Lucha contra la Pobreza, Carta Verde, Fortalecimiento de Consorcios de Riego y Agua Potable, Estrategia Agropecuaria, Rehabilitación y Mantenimiento de la Red Vial; Universalización de la Educación Básica, Red de Migración y el Centro de Formación Ciudadana de Tungurahua, Presa Mulacorral, Red Vial Provincial; Biblioteca de la ciudad y la provincia, Parque Provincial de la Familia, entre miles de obras que han potenciado nuestra provincia.

El H. Gobierno Provincial de Tungurahua se ha convertido en el actor primordial del cambio, es quien a través de su gestión ha vitalizado, respaldado y garantizado la ejecución de los procesos que nos han permitido ser una provincia diferente, ejemplo del país.

Misión

El H.G.P.T. tiene como visión ser coordinador, orientador, facilitador, planificador y ejecutor de acciones mancomunadas con gobiernos locales, instituciones públicas, privadas y organizaciones sociales, en los niveles:

parroquiales, cantonales, provincial, regional, nacional e internacional; con el fin de impulsar las iniciativas de desarrollo económico, social, ambiental y territorial de Tungurahua, bajo los principios de participación, mancomunidad, equidad, ética, efectividad y transparencia.

Visión Provincial

La Provincia de Tungurahua es un territorio productivo, competitivo, moderno y ambientalmente sano, que potencia los recursos existentes; posicionándose como una de las provincias más competitivas del país; proceso basado en los direccionamientos del Nuevo Modelo de Gestión y en sus principios de gobernabilidad, corresponsabilidad y representatividad.

Visión Institucional

El H. Gobierno Provincial de Tungurahua se constituye en uno de los líderes de desarrollo integral de la provincia, en su condición de referente político – técnico, con capacidades para orientar las grandes decisiones de interés provincial.

2.2.3 Gráficos de Categorías Fundamentales

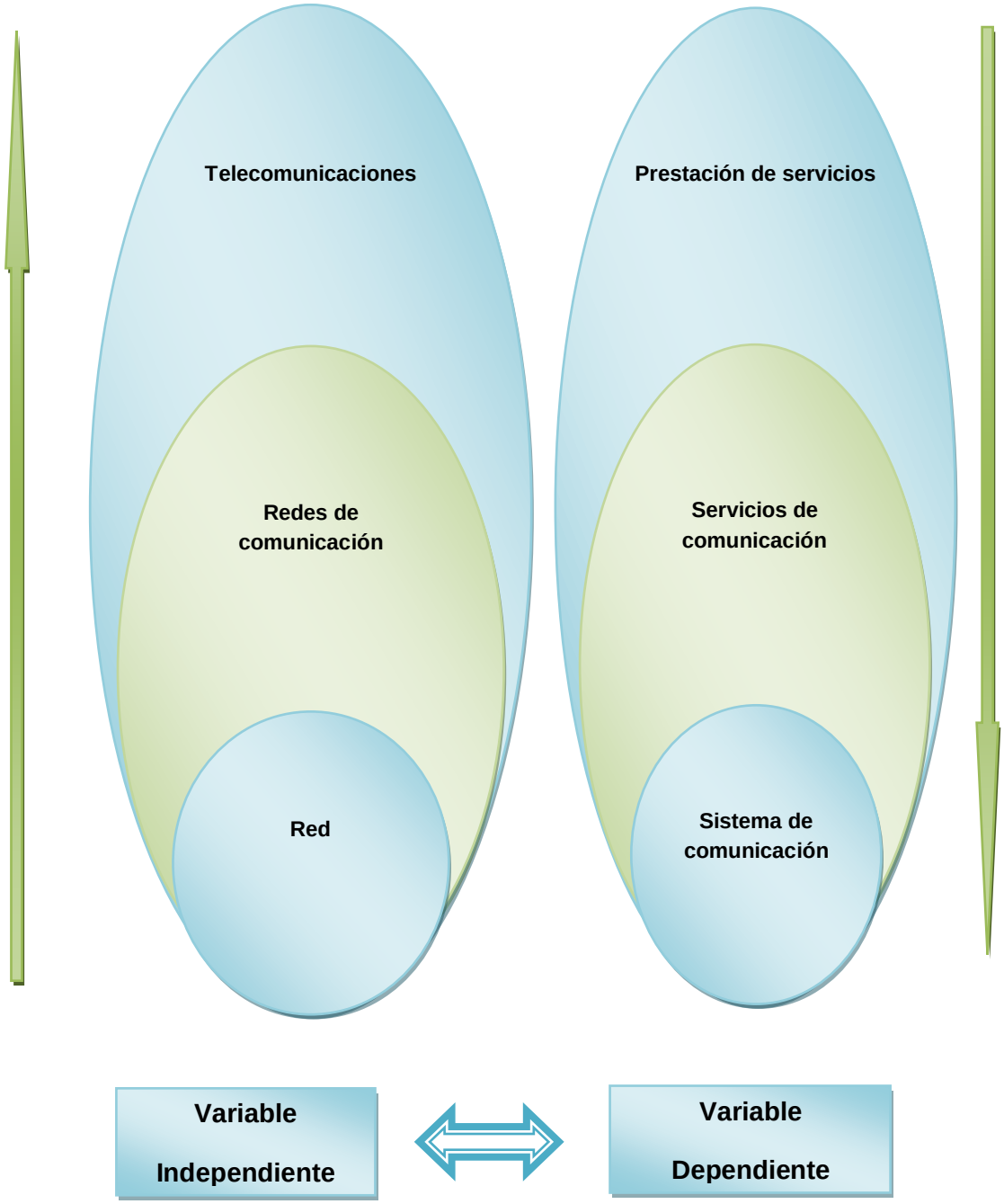
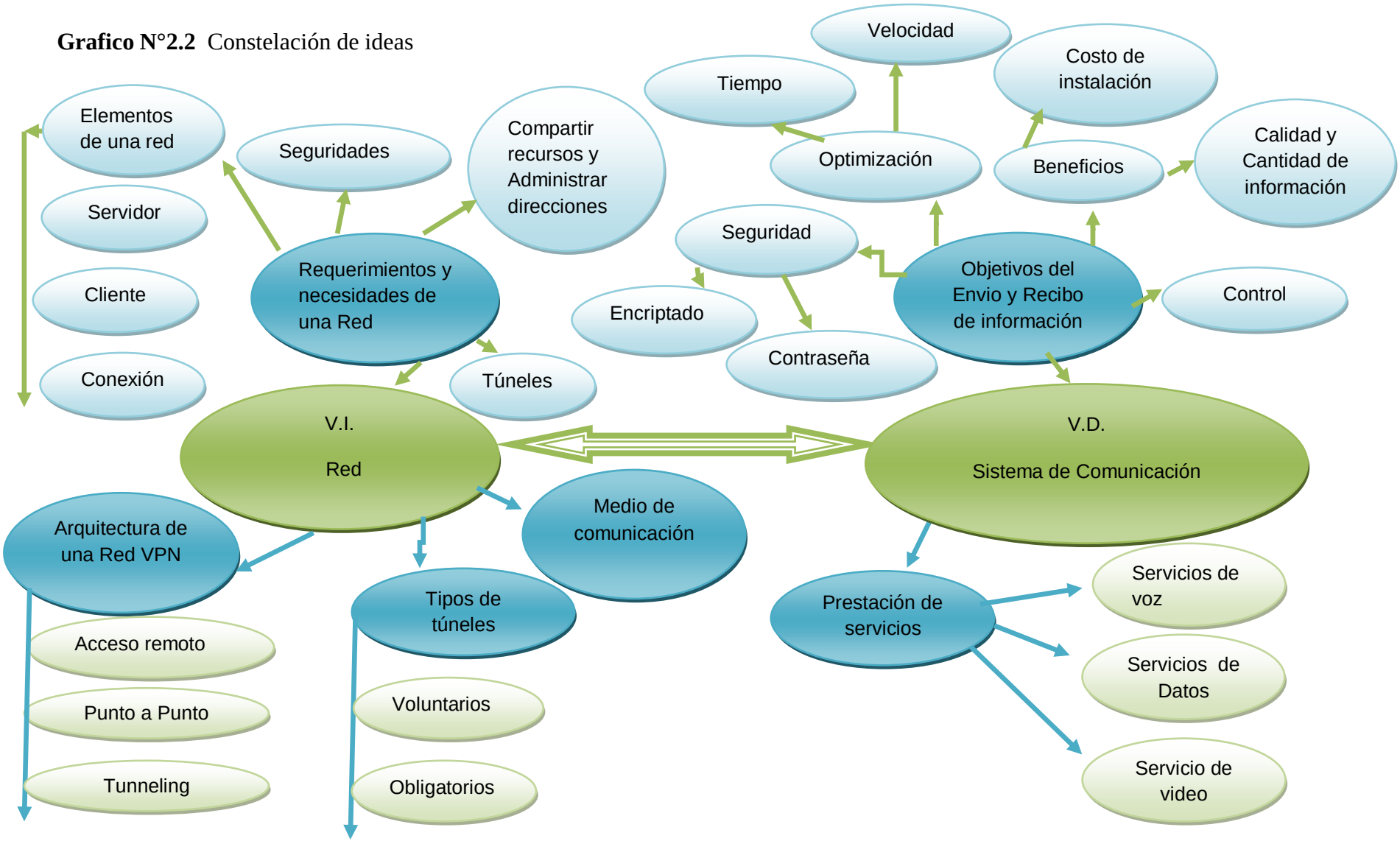


Grafico N°2.1 Categorías Fundamentales

Elaborado por: El Investigador

Subordinación Conceptual

Grafico N°2.2 Constelación de ideas



2.3 CATEGORÍAS FUNDAMENTALES

2.3.1 Telecomunicaciones

Las Telecomunicaciones, es toda emisión o recepción de señales signos, datos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través cables o en forma inalámbrica.

Las telecomunicaciones es una técnica que consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. Los elementos que integran un sistema de telecomunicación son un transmisor, un medio de transmisión y un receptor.

2.3.1.1 Clasificación de las Telecomunicaciones

Las telecomunicaciones se clasifican según su medio de propagación de las cuales tenemos:

- **Telecomunicaciones terrestres.-** Las telecomunicaciones terrestres tienen su medio de propagación son líneas físicas, (cables de cobre, fibra óptica, cable coaxial, cable multipar, etc.), ejemplo las líneas telefónicas.
- **Telecomunicaciones radioeléctricas.-** Las telecomunicaciones Radioeléctricas tienen como medio de propagación la atmósfera terrestre, realizando la transmisión de las señales de ondas; como por ejemplo las ondas de radio.
- **Telecomunicaciones satelitales.-** Las telecomunicaciones Satelitales tienen como medio de propagación la atmósfera terrestre y parte del espacio exterior, es decir las diferentes capas de la atmósfera hasta llegar a la órbita geosíncrona ubicada a 36000 Km. Sobre el nivel del mar; un ejemplo son los enlaces VSAT

2.3.2 Redes de comunicación

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.

Para establecer comunicación es necesario disponer de: Acceso a la red de comunicaciones, el transporte de la información, 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

Las redes de comunicación no son más que la posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital o un medio de transmisión de la era de la información.

Las Redes de comunicación nos permites la interconexión y por consiguiente mantener una comunicación con uno o varios usuarios ya sea de manera física por medio de cables o inalámbricamente.

MEDIOS DE TRANSMISIÓN

El medio de transmisión es el soporte físico que facilita el transporte de la información. Es una parte fundamental en la comunicación de datos. La calidad de la transmisión dependerá de sus características; Existen dos medios de transmisión los cuales son los medios guiados y los medios no guiados

2.3.2.1 Medios Guiados

Es cuando se tiene un medio físico a través de cual se propaga la información , las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

Los principales medios guiados son:

- Par trenzado (UTP, STP)
- Fibra óptica
- Cable coaxial

Par Trenzado

El par trenzado consiste en dos cables de cobre aislados y trenzados para reducir la interferencia eléctrica externa y de pares adyacentes. Dos cables paralelos forman una antena. Si se trenzan se reduce la diafonía. Existen algunos tipos como son el cable UTP, cable STP, etc.

Fibra Óptica

La fibra óptica es una delgada hebra de vidrio o silicio fundido que conduce la luz. Se requieren dos filamentos para una comunicación bi-direccional: transmisor y receptor. El grosor del filamento es comparable al grosor de un cabello humano, es decir, aproximadamente de 0,1 mm. Un cable de fibra óptica está compuesto por: Núcleo, manto, recubrimiento, tensores y chaqueta.

Cable Coaxial

El cable Coaxial consiste de dos conductores, pero es construido de manera diferente para operar sobre un rango más alto de frecuencias. Un cable coaxial sencillo tiene un diámetro de 0.4 a 1 pulgada.

Su estructura consta con una vaina externa que es un aislador plástico que evita el desgaste ante la lluvia y la erosión; una malla que su función es evitar la interferencia electromagnética; y un dieléctrico que da la eficiencia del cable coaxial, mientras más puro sea es mejor y su función es impedir el paso de los electrones.

2.3.2.2 Medios No Guiados

Los medios de transmisión no guiados son los que no confinan las señales mediante ningún tipo de cable, sino que las señales se propagan libremente a través del medio. Entre los medios más importantes se encuentran el aire y el vacío. Tanto la transmisión como la recepción de información se llevan a cabo mediante antenas

Los medios no guiados se refieren a los sistemas inalámbricos o redes inalámbricas.

Red inalámbrica

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, el alcance y la velocidad de sus transmisiones.

Algunos de los medios Guiados son:

1. Guía de onda

La guía de onda es un medio hueco en su interior construido de aluminio con una impedancia característica de 500 ohms. Tiene tres modos de transmisión: Transversal Eléctrico (natural 10), Transversal Magnético, y Transversal Electromagnético.

Existen generalmente de dos tipos que son guías de ondas cilíndricos y guías de ondas rectangulares.

Una guía de onda sirve para la construcción de antenas y se la aplica en microondas, por lo cual la polarización es un factor importante ya que nos indica el comportamiento del campo eléctrico. La desventaja de una guía de onda es que soporta hasta 70 millas/hora el viento

2. Ondas de Radio

Las ondas de radio son un medio de transmisión que ocupan el aire como medio de propagación, su rango de frecuencias es de 30 MHz a 1 GHz. Sirve para la transmisión de voz, datos, televisión, radio y utiliza antenas omnidireccionales. La frecuencia se divide en bandas para los radioaficionados: A, B y C.

3. Microondas

Las microondas es un medio que permite la transmisión de un punto a otro. Opera en frecuencias mayores a 1 GHz. Las frecuencias de 2 a 4 GHz se dividen en sub bandas: L, X. y emplea antenas direccionales, de rejillas, offset, y parabólicas.

Es necesario tener línea de vista y su confiabilidad es del 99% y tiene un retardo de 5 mseg. El uso principal de los sistemas de microondas terrestres son los servicios de telecomunicación de larga distancia

4. Satélites

Un satélite es un sistema electrónico complejo que se encuentra en la zona geoestacionaria o geosíncrona, ubicado a una altura de 36000 Km en la Troposfera, el mismo que debe ponerse en sincronía con la rotación de la Tierra girando a 6879 millas/hora.

Tiene una frecuencia ascendente (uplink) y descendente (downlink). La frecuencia de subida es siempre mayor que la frecuencia de bajada debido a la presión presentada en la atmósfera[1]

[1] http://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

2.3.3 Sistemas de comunicación

"Un sistema de comunicación es el conjunto de equipos y enlaces tanto físicos como electromagnéticos, utilizables para la prestación de un determinado servicio de telecomunicaciones".

2.3.3.1 Elementos de un sistema de comunicación

En toda comunicación existen tres elementos básicos en un sistema de comunicación: el transmisor, el canal de transmisión, el receptor, y el transductor como se muestra en el Gráfico 2.3.

El Transmisor: El Transmisor pasa el mensaje al canal en forma de señal, su operación más importante es la modulación, o acoplamiento de la señal transmitida a las propiedades del canal por medio de una onda portadora.

El Canal de Transmisión: El canal de transmisión es el medio por el que se realiza el **nexo eléctrico** entre al transmisor y el receptor. A medida que la distancia entre la fuente y el destino aumenta, se produce la atenuación de la potencia de la señal, por lo que debe compensarse en el receptor mediante un amplificador para ser recibida correctamente

El Receptor Su función es extraer del canal la señal transmitida, la operación central que realiza es la demodulación (proceso inverso a la modulación). Además, como las señales son frecuentemente débiles debido a la atenuación, el receptor debe tener varias etapas de amplificación.

El transductor El transductor es un dispositivo que cambia una forma de energía por otra. Pueden convertir lo que oímos, vemos y decimos en señales que permiten el procesamiento, almacenamiento y transmisión de la información.[2]

[2] http://www.slideshare.net/mamogetta/sistema-de-comunicacin-redes-de-telecomunicaciones-presentation

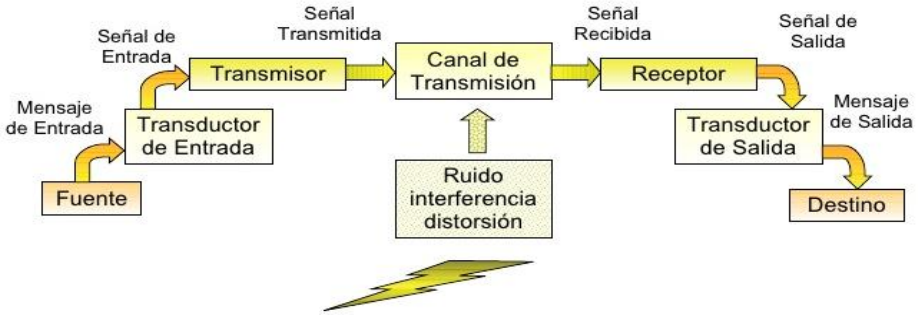


Gráfico Nº 2.3 Sistema de comunicaciones

FUENTE: http://www.slideshare.net/mamogetta/sistema-de-comunicacin-redes-de-telecomunicaciones-presentation

2.3.4 Red Privada Virtual (VPN)

Como se muestra en el Grafico 2.4 una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura[3]

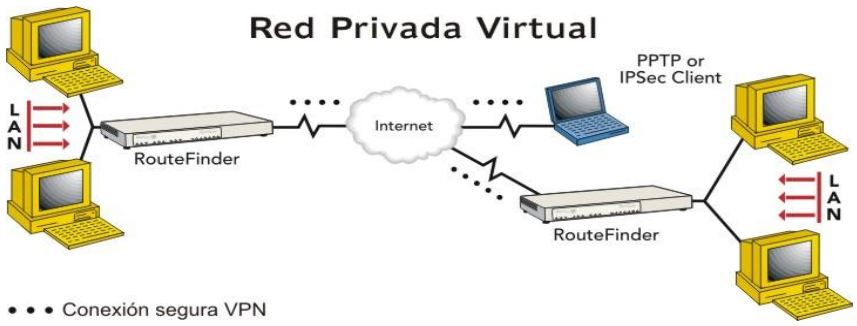


Gráfico Nº 2.4 Red privada virtual

FUENTE: http://tescoredes.wordpress.com/2011/05/29/

[3] http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp

2.3.4.1 Necesidades y surgimiento de las VPN

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de email, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa

2.3.4.2 **Elementos de una VPN**

Los elementos que conforman una red privada virtual son:

Servidor VPN. Un servidor VPN es una computadora que acepta conexiones VPN de clientes VPN. Un servidor VPN puede proporcionar una conexión de acceso remoto VPN o una conexión de enrutador a enrutador.

Cliente VPN. Un cliente VPN es una computadora que inicia una conexión VPN con un servidor VPN. Un cliente VPN o un enrutador tiene una conexión de enrutador a enrutador.

Túnel. Un Túnel es la porción de la conexión en la cual sus datos son encapsulados.

Conexión VPN. La conexión VPN es la porción de la conexión en la cual sus datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma porción de la conexión.

El esquema de una conexión VPN se muestra en el Gráfico 2.5.

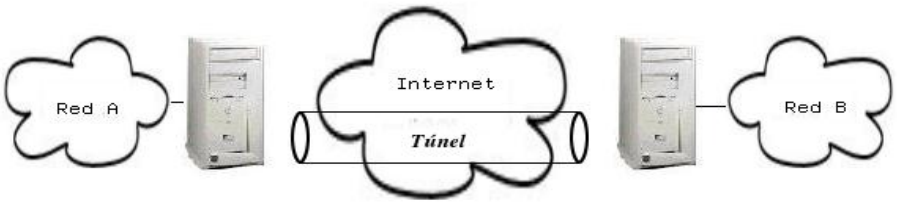


Gráfico Nº 2.5 Esquema de una VPN a través de Internet
FUENTE: http://blackspiral.org/docs/pfc/itis/node5.html

2.3.4.3 Requerimientos indispensables de una VPN

Los requisitos indispensables para implantar una VPN son:

Políticas de seguridad: Codificación de datos (los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red), administración de claves (la VPN debe generar y renovar las claves de codificación para el cliente y el servidor.)

Requerimiento de aplicaciones en tiempo real: Envío de resultados a tiempo, es necesario que las operaciones que se realicen sean correctas para garantizar que la información llegue en el tiempo requerido.

Compartir datos, aplicaciones y recursos: Compartir información, es indispensable poder enviar y recibir datos entre los miembros de la red ya sea voz datos o video.

Servidor de acceso y autenticación (identificación de usuarios): debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren los accesos, la información y el instante en que se realizó.

Administración de direcciones: La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Soporte a protocolos múltiples: La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet(IP), el intercambio de paquete de internet(IPX) entre otros.[4]

2.3.4.4 Tipos de VPN

Existen Tres tipos de sistemas VPN que son:

Sistemas Basados en Hardware

Los sistemas basados en hardware, son eficientes y seguros, requieren de una configuración correcta y lista.

La implementación entre ROUTERS provee la capacidad de asegurar un paquete en una parte de la red, esta seguridad se logra a través del TUNNELING de paquetes.

Sistemas Basados en Firewall

Estas VPN se los utiliza con un software de cortafuegos (firewall). Aprovechan las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autentificación fuerte.

Sistemas Basados en Software

Estos sistemas basados en software son utilizados en el caso de que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma empresa.

[4] http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1874

2.3.4.5 Arquitectura de una VPN

Básicamente existen tres arquitecturas de conexión VPN que son:

VPN de acceso remoto

VPN de acceso remoto es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etc.) utilizando Internet como vínculo de acceso asi como se muestra en el Gráfico 2.6. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

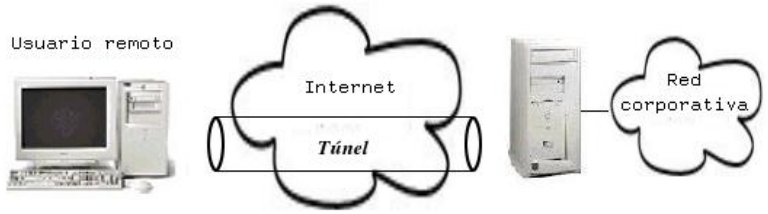


Gráfico Nº 2.6 Esquema de una VPN de acceso remoto
FUENTE: http://blackspiral.org/docs/pfc/itis/node5.html

- **VPN punto a punto**

Una VPN punto a punto se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Como se muestra en el grafico 2.7 los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

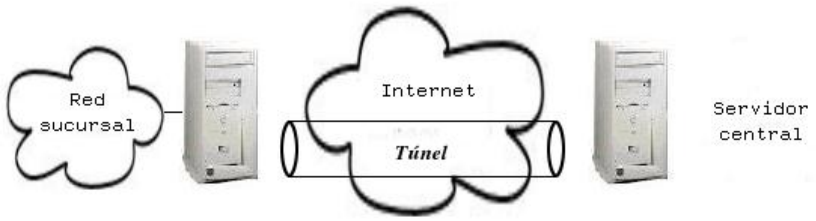


Gráfico Nº 2.7 Esquema de una VPN punto a punto
FUENTE: http://blackspiral.org/docs/pfc/itis/node5.html

- **Tunneling**

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo un PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

- **VPN over LAN**

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la 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 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 inalámbricas (WiFi).Este esquema se lo Observa en el Gráfico 2.8

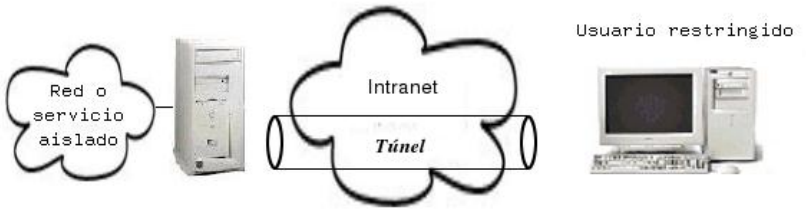


Gráfico Nº 2.8 Esquema de una VPN interna
FUENTE: http://blackspiral.org/docs/pfc/itis/node5.htm

2.3.4.6 Túneles

Un sistema de túnel es un método que transforma las tramas (o paquetes) de información confidencial para que estas no sean leídas por terceros que estén presentes en el medio de transmisión. Este túnel como vemos en el Gráfico 2.9 es creado en forma virtual sobre el trayecto de red que es considerado público, es decir las tramas quedan indescifrables para los usuarios de la red pública y realizan la trayectoria sin que estas sean perturbadas creando un camino inviolable.

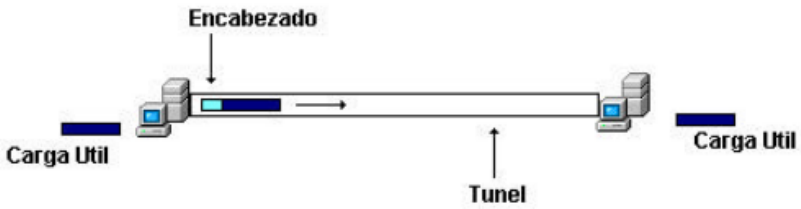


Gráfico Nº 2.9 Túnel
FUENTE: http://cybertesis.uach.cl/uach/2004/bmfcil732/bmfcil732p.pdf

2.3.4.7 Tipos de Túneles

Hay dos tipos de túneles los voluntarios y los obligatorios.

· **Túneles voluntarios**: Un túnel voluntario es cuando un PC de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, el PC del usuario es un punto terminal del túnel y actúa como un cliente del túnel.

· **Túneles obligatorios**: Un túnel obligatorio es cuando un servidor de acceso de marcación, capaz de soportar una VPN, configura y crea un túnel obligatorio. Con un túnel obligatorio, el PC del usuario deja de ser un punto terminal del túnel. [5]

2.3.4.8 Protocolos o tecnologías utilizados para VPN-IP

En una red VPN es de suma importancia la seguridad para su correcto funcionamiento, para ello se han creado varios protocolos como vemos en la figura 2.10 continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro.

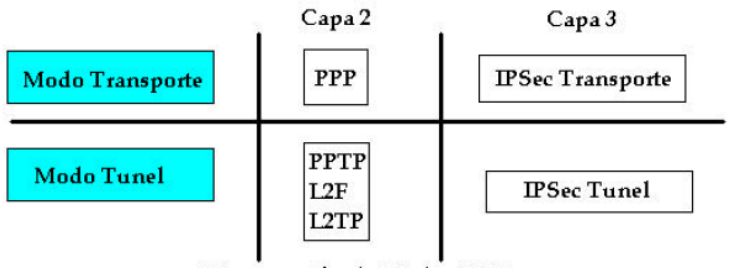


Gráfico Nº 2.10 Protocolos VPN-IP.
FUENTE:http://cybertesis.uach.cl/uach/2004/bmfcil/doc/bmfcil732p.pdf

2.3.4.9 Protocolos de túnel

Las tres alternativas protocolares relevantes para lograr un enlace de túnel en una red de comunicación que requiera seguridad y confidencialidad, son las que se observa en el figura 2.11

[5] http://blackspiral.org/docs/pfc/itis/node5.html , http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1875

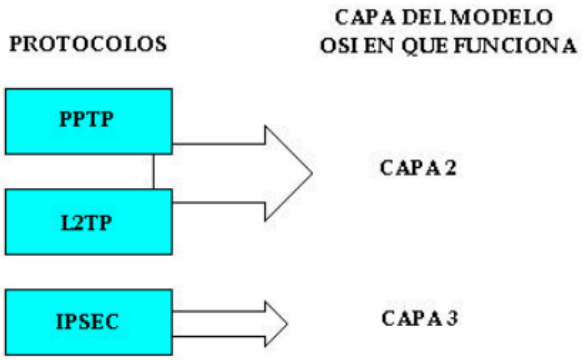


Gráfico Nº 2.11 Protocolo VPN en el modelo de referencia OSI
FUENTE: http://cybertesis.uach.cl/uach/2004/bmfcil/doc/bmfcil732p.pdf

2.3.4.10 Protocolos de túnel VPN

Los protocolos consisten en el establecimiento de túneles mediante la utilización de encapsulado y encriptación de las tramas, de esta forma se establece un enlace punto a punto privado y seguro sobre la infraestructura pública que está siendo utilizada. Para cumplir las necesidades de seguridad se establecieron los siguientes protocolos:

a) **PPTP (Point to Point Tunneling Protocol)**

PPTP Permite el tráfico seguro de datos desde un cliente remoto hasta un servidor corporativo privado, estableciéndose gracias a este la red privada virtual basada en TCP/IP.

PPTP soporta múltiples protocolos de red como IP, IPX o Net BEUI que comúnmente transitan sobre las redes públicas como Internet y puede ser utilizado para crear VPN sobre otras redes públicas o privadas como líneas telefónicas (PSTN acceso telefónico a redes), redes LAN y WAN, Internet u otras redes públicas basadas en TCP/IP y además aprovecha las ventajas de los mecanismos de autenticación, compresión y cifrado de las tramas de información.

b) **L2TP (Protocolo túnel de capa 2)**

Al igual que PPTP este protocolo utiliza la trama PPP creada al conectar Cliente – ISP, donde luego se realiza el túnel de capa 2, funcionando de modo bastante similar teóricamente al protocolo antes mencionado. Sin embargo, este sistema ofrece más seguridad a los datos de información que viajan por el medio inseguro. L2TP es un híbrido entre PPTP y L2F y adquiere lo mejor de cada protocolo

c) **IPSec (Protocolo de seguridad para redes IP)**

Protocolo de seguridad en Internet. Este protocolo es en realidad un conjunto de estándares lo cual asigna al sistema donde se implementa servicios criptográficos de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa 3 de red de OSI, de tal forma que su funcionamiento es bastante transparente al momento de llegar al nivel de aplicación, es decir se puede trabajar con HTTP, FTP, Telnet, SMTP, etc. IPSec es poderoso en comparación a las otras alternativas de túneles de seguridad.[6]

2.3.5 Red

Una red es una serie de ordenadores y otros dispositivos conectados por cables entre sí., esta conexión les permite comunicarse entre ellos y compartir información y recursos.

Las redes varían en tamaño; pueden reducirse a una oficina o extenderse globalmente.

Una red conectada en un área limitada se conoce como Red de área local (LAN). Una LAN está contenida a menudo en una sola ubicación. Una Red de área extensa (WAN) es un grupo de dispositivos, o varias LAN, conectados en una área geográficamente mayor, a menudo por medio de líneas telefónicas u otro

[6] http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/doc/bmfcil732p.pdf

formato de cableado como puede ser una línea dedicada de alta velocidad, fibra o enlace vía satélite. Una de los mayores ejemplos de WAN es la propia Internet[7]

2.3.6 Prestación de Servicios

"Se le puede definir que es similar a un contrato mediante el cual una persona, normalmente un profesional en cualquier área que se desempeñe, se compromete con respecto a otra a realizar una serie de servicios a cambio de un precio. Es importante señalar que el pago es dirigido al cumplimiento de metas, horas, objetivos, proyectos; etc. el incumplimiento de dichas metas no obliga al pago Proporcional"[8]

También se considerará prestación de servicios el suministro de productos o equipos que hayan sido confeccionados o adquiridos, previo encargo de su destinatario conforme a las especificaciones de éste, así como aquellos otros que sean objeto de adaptaciones sustanciales necesarias para el uso por su destinatario Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet dando así la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitiendo a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

2.3.7 Servicios de comunicación

"Básicamente es el Intercambio, sobre algún medio de transmisión (guiado o no guiado), de información codificada que ha sido o va a ser procesada por algún sistema informático, que las empresas ofrecen este servicio según los requerimientos de comunicación del cliente".[9]

[7] http://jorge429.files.wordpress.com/2009/08/resumen-la-red.doc
[8] http://repo.uta.edu.ec/bitstream/handle/123456789/405/Tesis_t626ec.pdf?sequence=1
[9] http://repo.uta.edu.ec/bitstream/handle/123456789/405/Tesis_t626ec.pdf?sequence=1

2.3.8 Servicios triple Play

Identifica la prestación de los servicios de voz, Datos y video sobre una infraestructura común de transmisión de datos o IP.

2.3.9 Descripción de los servicios

Servicio de Datos. Servicio de datos se caracteriza por requerir unos anchos de banda bastante elevados. La pérdida de paquetes le afecta, pero es capaz de recuperarse ante estos efectos, y es totalmente inmune ante retardos o jitter. Si alguien se conecta a una página Web (típico servicio de datos), si esa página tarda en cargarse 5 ó 6 segundos, aunque es algo que puede desesperar al usuario, en realidad la información se va a poder recibir correctamente y se va a poder interactuar con ella.

Servicio de Voz. El servicio de voz se suele caracterizar por tener un ancho de banda bastante reducido. Si se usa el codec básico G.711, la tasa de bits será de 64 kbps, pero si se usan codecs más avanzados, esta tasa se puede reducir hasta los 4 kbps.

Servicio de Vídeo. En el servicio de video se transmiten grandes volúmenes de datos y, además, suele presenta ciertos requisitos sobre el jitter y los retardos. Por ejemplo, las distintas pantallas se deben poder refrescar adecuadamente. Tradicionalmente este servicio suele ir acompañado de audio o de voz, con lo que además se necesita cierta sincronización entre el audio y el vídeo. No sería aceptable que a la mitad de una película se escucharan los sonidos de una escena cuyas imágenes aparecen más tarde.[10]

[10] http://www.ramonmillan.com/documentos/tripleplay.pdf

2.4 Hipótesis

¿La subutilización de la red genera un deficiente sistema de comunicación entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas?

2.5 Señalamiento de Variables

- **Variable Independiente:** Red
- **Variable Dependiente:** Sistema de Comunicación

CAPITULO III

METODOLOGÍA

3.1 Enfoque de la Investigación

La conexión VPN para acceso remoto entre el edificio del H. Gobierno Provincial de Tungurahua y sus bodegas ubicadas en el sector de Catiglata se desarrollo con un enfoque cuali-cuantitativo debido a que se utilizo tanto técnicas cualitativas como cuantitativas, orientado a identificar y comprender las causas de la deficiencia en la comunicación objeto que se estudió con lo cual se obtuvo los resultados deseados.

Es una forma de describir e interpretar la realidad del problema existente en el H.G.P.T, en un espacio contextualizado con una perspectiva tanto desde adentro como de afuera lo que orienta hacia la verificación de la hipótesis, pone en énfasis el proceso de investigación, formula una hipótesis lógica que será resuelta en base de interrogantes.

3.2 Modalidad Básica De Investigación

La investigación realizada tiene las modalidades de investigación documental e investigación de campo

3.2.1 Investigación documental o bibliográfica

Esta investigación es documental bibliográfica porque se busco información en libros, informes y revistas ya que se tuvo como propósito detectar, profundizar y ampliar diferentes enfoques, teorías, conceptualizaciones y criterios, basándose en documentos de redes privadas virtuales

3.2.2 Investigación de Campo

Esta se baso en el estudio de los hechos en el edificio del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas en Catiglata en donde se produjeron los acontecimientos, aquí se tuvo contacto en forma directa con la realidad, con lo cual se obtuvo información de acuerdo con los objetivos del proyecto.

3.3 Tipos De Investigación

Esta investigación tuvo un nivel **exploratorio** pues se reconoció las variables que nos competen a las cuales se dio una mayor amplitud y dispersión. Un nivel **descriptivo** que permitió dar pronósticos básicos, para lo cual fue necesario tener un conocimiento suficiente de la situación.

3.4 Población Y Muestra

3.4.1 Población

Tabla 3.1: Población

Cargo	Nº de personas
Administrador	1
Soporte	1
Proyectos	1
Asesor	1
Total	4

Elaborada por: El investigador

3.4.2 Muestra

En consideración al tamaño de la población se va a trabajar con todos sus componentes, es decir el total del personal del departamento de sistemas del HGPT será tomado como muestra.

3.5 Operacionalización de Variables

Tabla 3.2. Operacionalización de la variable independiente: Red

CONCEPTO	CATEGORIAS	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS INSTRUMENTALES
Red: Una red Virtual es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet dando así la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo una red local o el Internet	Tecnología de red Red local Red publica Internet	Equipos Tecnología Protocolos Conexión	¿En qué estado se encuentran los equipos de comunicación del H.G.P.T? ¿Con que tipo de tecnología cuenta el edificio central para la transmisión de información con sus bodegas? ¿Qué protocolos de comunicación se utiliza en la conexión con las bodegas? ¿Qué eficiencia tiene la conexión que existe entre el edificio central y las bodegas del GOBIERNO PROVINCIAL?	Observación: Mediante la guía de observación en las instalaciones del H. GOBIERNO PROVINCIAL DE TUNGURAHUA Entrevista: Dirigida al Administrador del H. GOBIERNO PROVINCIAL DE TUNGURAHUA

Elaborado por*:* El Investigador

Tabla 3.3. Operacionalización de la variable dependiente: Sistema de Comunicación

CONCEPTO	CATEGORIAS	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS INSTRUMENTALES
Sistema de comunicación: Permite el Envío y recepción datos de manera ordenada y sincronizada brindando servicios como: servicios de voz, datos y video, sobre una infraestructura común de transmisión de datos o IP.	Envío y recepción de información Prestación de servicios Internet Transmisión de datos IP	Ancho de banda Seguridad Información Red	¿Posee el H.G.P.T el ancho de banda necesario para abastecer su sistema de comunicación? ¿Cuál es el nivel de seguridad de los sistemas de comunicación del departamento de sistemas del H.G.P.T para él envió y recepción de información? ¿Dispone el GOBIERNO PROVINCIAL DE TUNGURAHUA con el personal capacitado para administrar este tipo de red? ¿Qué beneficios traerá la implementación de la red?	Observación: Mediante la guía de observación en las instalaciones del H. GOBIERNO PROVINCIAL DE TUNGURAHUA Entrevista: Dirigida al Administrador del H. GOBIERNO PROVINCIAL DE TUNGURAHUA

Elaborado por: El Investigador

3.6 Recolección de la Información

Para el plan de recolección de la información con lo cual se sustento la investigación, se realizó estrategias para que sea oportuna y adecuada.

En primera instancia se expreso claramente los objetivos, que se lograron con la investigación y con el apoyo de los miembros del departamento de sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus directivos.

Se realizo básicamente un estudio de los indicadores que se mencionan en cada una de las matrices de la Operacionalización de las variables, las mismas que se estudiaron para conocer si estos factores intervinieron en la problemática que se produjo en las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA.

Esta investigación tuvo como propósito investigar las diferentes causas que produjeron la no comunicación entre las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA en Catiglata con su edificio principal, con el fin de plantear una conexión adecuada conjuntamente con el departamento de sistemas para así mejorar la seguridad y el control de los procedimientos que se suscitan en sus bodegas.

Para el presente proyecto se empleó las técnicas de **observación** y **entrevista**, ya que estas permitieron estar en el lugar de la problemática y tomar la información necesaria para la investigación.

La investigación efectuada se realizó por Daniel Portero, el mismo que se encargo de la recolección de información para el establecimiento de este proyecto.

Tabla 3.4. Plan de recolección de información

Preguntas Básicas	
¿Para qué?	Lograr los objetivos planteados con la empresa.
¿De qué personas u objetos?	Funcionarios e instalaciones del H. GOBIERNO PROVINCIAL DE TUNGURAHUA
¿Sobre qué aspectos?	Indicadores que se menciona en cada una de las matrices de la Operacionalización de las variables
¿Quién lo investigara?	Daniel Portero
¿Cuándo?	6 Meses después de su aprobación
¿Dónde?	Departamento de sistemas y Bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA
¿Cuántas veces?	Las necesarias
¿Qué técnicas de recolección?	Observación y Entrevista
¿Con qué?	Guías de Observación y Entrevista

Elaborado por*:* El Investigador

3.7 Procesamiento Y Análisis

Luego de haber obtenido la información se realizó un proceso de revisión y análisis de datos para procesar los trabajos de observación y entrevista realizados, hacer una tabulación en base a ello y así emitir un resultado de lo investigado.

Esto permitió dar criterios para sustentar los resultados generados.

Se revisó la información de la observación y la entrevista realizadas para evitar que exista información que no corresponda, o que se encuentren incompletas o contradictorias.

3.7.1 Plan de Análisis e Interpretación de Resultados

La observación permitió dar un criterio para sustentar la realidad de la entidad, destacando tendencias relacionadas fundamentalmente de acuerdo con los objetivos e hipótesis.

Se realizó una revisión de las respuestas recopiladas tanto de la observación como de la entrevista efectuada en las instalaciones del H.G.P.T, con esto se pudo saber las verdaderas necesidades de esta entidad lo que sirvió para la implementación del proyecto.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis e Interpretación de Resultados

En este capítulo la información recolectada fue analizada de acuerdo a la observación y entrevista que se realizo en las instalaciones del H.G.P.T., con lo cual se procedió a interpretar los resultados obtenidos.

La información obtenida fue tabulada y analizada de forma sistemática de acuerdo a las preguntas planteadas, además interpretados de acuerdo a la parte técnica.

Es importante señalar que la unidad de sistemas informáticos esta bajo la dependencia de la Dirección Administrativa, la cual realiza las actividades de unidad técnica sobre la tecnología que abarca esta rama.

Entrevista dirigida al administrador del departamento de sistemas del HGPT

Entrevista Nº 1

¿En qué estado se encuentran los equipos de comunicación del departamento de sistemas del H.G.P.T?

Tabla Nº 4.1 Estado de los equipos de comunicación

Nº	Tipo	Cant.	Nombre	Descripcion	Rendimiento
1	Switch capa 3	1	Cisco Catalyst 3560G -48PS	48 puertos	100%
2	Switch capa 2	2	3COM SuperStak 3 Switch 4226T	24 puertos	100%
		2	3COM SuperStak 3 Switch 3300XM	24 puertos	0%
3	Switch capa 1	3	Hub Generic		100%
4	Servidores	1	Sunfirev120	Servidor Proxi de internet	100%
		1	Sunfire280r	Servidor Correo electrónico	90%
		1	SunfireV440	Servidor base de Datos	90%
		1	ServerHCTP	Dominio, DNS y Antivirus	90%
		1	ServidorDF	Servidor Servicio Contable	50%
		1	Servidor HP	Aplicación mapeo de actores	50%
5	Firewall	1	Symantec Gateway Security	Protección	70%
6	Modem	1	Huawei SMARTAX MT 800	Conexión ADSL	100%
7	Acces point	10	Proxim ORINOCO A-4000	Acces P. 802.11g, 2,4 Ghz	90%
		4	TEW-430APB 802.11g Wireless	Acces P. 802.11g, 2,4 Ghz	75%
		3	Senao Internacional NCB-8610	Acces P. 802.11b, 2,4 Ghz	80%
		2	Links Waps 54G	Acces P. 802.11g, 2,4 Ghz	100%
8	Computadores	126	HP	Core 2Quad Win7 2.66Gz	95%
9	Laptps	7	Hp, Toshiba, hacer	Core2D, Core3, Core 5	100%
10	Roters	2	D-Link Dir 600, D-link 524 B		100%
11	Lineas telefonicas	3			100%

Fuente: Entrevista **Elaborado por**: Daniel Portero

Tabla Nº 4.2 Servidores

Servicio	Servidor	Plataforma Servidor	Plataforma Clientes
Firewall	Symantec Gateway Security	Linux	
Internet Compartido	Squid 3.0	Solaris 10	Windows 2000, XP, Vista,7
Correo electrónico	Lotus Domino 7.01	Solaris 10	Windows, Me,2000, XP, Vista, 7 Lotus Notes8
Antivirus	Symantec EndPoint Protection 11	Windows 2008 Enterprise	Windows 98, Me,2000, XP, Vista, 7
Controlador de Dominio	Active Directory	Windows 2008 Enterprise	Windows 98, Me,2000, XP, Vista, 7
DNS	DNS Server	Windows 2008 Enterprise	Windows 98, Me,2000, XP, Vista, 7
Adquisición de Materiales	base datos documentales de Lotus Domino	Solaris 9	Windows 98, Me,2000, XP, Vista, 7, Lotus Notes 8
Sistema de Control de Recursos Humanos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, 7. Clientes de la aplicación y Oracle
Sistema Médico Odontológico	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, 7. Clientes de la aplicación y Oracle
Sistema de Control de Proveedores	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, 7. Clientes de la aplicación y Oracle
Sistema Financiero FINANSG	Aplicación en Power Builder con base de datos de SQL 2005 Server	Windows 2008 Advanced Server	Windows 98, Me,2000, XP, Vista, 7. Cliente de la aplicación

Fuente: Entrevista **Elaborado por**: Daniel Portero

El nivel de calificación de los equipos se los dio según su desempeño en las instalaciones del H.G.P.T. Se le asigno un porcentaje de acuerdo a ciertas funciones que son:

Servidores: Proporción de información y recursos, Servicios a los clientes de red.

De 0 a 20% Mala (En desuso, Dañado, La información no llega)
De 20 a 50% Regular (Información Tardía e incompleta, Sistemas operativos antiguos, Firewall desactualizado)
De 50 a 80% Buena (Información tardía y completa, Sistemas operativos seguros, Firewall confiable)
De 80 a 100% Muy Buena (Información a tiempo y completa, Sistemas operativos seguros, Firewall actualizado)

En el HGPT los servidores que se tomaron en cuenta son los que brindan: la seguridad aplicada, el servicio de internet, el servicio de correo electrónico, el servicio de base de datos, el antivirus, y servicio contable.

El Servidor de internet tiene un desempeño del 100%, utiliza sistema operativo Solaris 10
El servidor de correo electrónico tiene una desempeño del 90%, utiliza sistema operativo Solaris 10.
El Servidor de base de datos tiene un desempeño del 90%, utiliza sistema operativo Solaris 10.
El servidor de Dominio, DNS, y antivirus tiene un desempeño del 90%, utiliza Windows 2008 Interprise
El servidor de sistema contable tiene un desempeño del 50%, utiliza Windows 2008 Advance Server.
El servidor de Aplicación Mapeo de Actores tiene un desempeño del 50%, utiliza Linux Fedora 9

Switchs: Conexión a la red Interna del HGPT, Estado físico, Capa del modelo OSI

De 0 a 20% Mala (En desuso, Dañado)
De 20 a 50% Regular (Puertos en mal estado, Perdida de Información)
De 50 a 80% Buena (Ciertos puertos Funcionando, Capa del modelo OSI 2)
De 80 a 100% Muy Buena (Puertos en perfecto estado, Capa del Modelo OSI 2 o 3)

Los Switchs que utilizan en el Gobierno Provincial dan conexión a la red de todos los departamentos tanto del edificio central como al edificio de servicios de la provincia con una topología estrella Extendida, y se encuentran en perfecto estado tanto físico como tecnológico ya que la capa 2 del modelo OSI permite dividir la red LAN en múltiples dominios de colisión, tienen capacidad Duplex, soporte VLAN, además el Switch de capa 3 tiene alimentación eléctrica por Ethrnet (POE) y soporta ruteo.

Routers: Conexión Inalámbrica, Estado físico.

De 0 a 20% Mala (En desuso, Dañado)
De 20 a 50% Regular (Puertos en mal estado, Wireless defectuoso)
De 50 a 80% Buena (Puertos funcionando, Wireless funcionando)
De 80 a 100% Muy Buena (Puertos en perfecto estado, Gran alcance del Wireless)
Los routers son de 4 puertos marcas D-LINK DIR600 y D-LINK 524B, utilizan IPs estáticas con lo cual proveen de internet inalámbrico a 3 computadores portátiles del departamento de sistemas, tiene un desempeño del 100 % ya que son nuevos, además brindan conexión al Switch que interconecta los 2 Edificios del Gobierno Provincial de Tungurahua

Las computadoras se les da ese porcentaje por su tiempo de adquisición, fueron compradas en al año 2009 son marca Hp tienen procesador CORE 2 Quad, 2.66Ghz de velocidad, y sistema operativo Windows 7.
Las laptops del departamento de sistemas tienen un correcto desempeño ya que son maquinas actuales, son de marcas Hp CORE 2DUO, Toshiba CORE 5 y Acer CORE 3.

Los equipos de la institución se encuentran en un estado apto para dar un buen funcionamiento a la comunicación y a la red de la misma, el único inconveniente fue el sistema operativo que podría ser actualizado y así el desempeño podría ser del 100% lo cual sería de mucha ayuda para el HGPT.

Fuente: Entrevista
Elaborado por: Daniel Portero

Entrevista Nº2

¿Posee Ancho de banda necesario para abastecer su sistema de comunicación?

El ancho de banda que le provee la empresa proveedora de internet que en este caso es CNT es de 2 Mbps de bajada y 512Kbps de subida utilizando un Router D-LINK 524B ADSL, con lo cual el sistema de comunicación funciona perfectamente, con una dirección IP pública de 200.107.35.65 con máscara de red 255.255.255.248, es decir, se posee un rango de 6 IPs públicas 200.107.35.64/29

La red interna tiene una dirección de red 192.168.1.0 con máscara de red 255.255.255.0 lo que se denomina una red plana, esto ocasiona que los paquetes informáticos que se generan sean difundidos a todos los dispositivos de la red.

Fuente: Entrevista
Elaborado por: Daniel Portero

Entrevista Nº3

¿Qué Beneficios traerá la implementación de la Conexión VPN?

Una Conexión VPN permitirá que se mejore diferentes aspectos en el H.G.P.T como: optimización en los recursos como la utilización de cables que elevan los costos de la red, la seguridad en él envió y recibo de información, el cuidado y control tanto de los empleados como de los equipos que se almacenan en las bodegas y la comunicación entre las bodegas y el edificio principal.

Fuente: Entrevista
Elaborado por: Daniel Portero

Entrevista Nº4

¿Cuál es el nivel de conocimiento del personal del departamento de sistemas para administración de una VPN?

El departamento de sistemas del H.G.P.T esta formado por 3 ingenieros en sistemas y un técnico electrónico con los conocimientos necesarios para mantener en funcionamiento y dar mantenimiento esta red.

Fuente: Entrevista
Elaborado por: Daniel Portero

Observación realizada en las instalaciones del HGPT

Observación Nº1

Tecnología con la que cuenta el edificio central para la transmisión de información con sus bodegas

Tabla Nº 4.3 Tecnología

Tipo de tecnología	Velocidad de Trasmisión
Conexión Remota	2Mbps
Radio Enlace Spread Spectrum (Dañado)	10Mbps

Fuente: Observación

Elaborado por: Daniel Portero

Cuenta con conexión mediante internet, es decir conexión remota con una velocidad de 2Mbps que provee la compañía proveedora de internet CNT.
También cuenta con una conexión mediante red telefónica que le provee CNT.
Había un radio enlace con tecnología Spread Spectrum con lo cual se asegura la confidencialidad de la información transmitida gracias a la Multiplexación por división de código, lamentablemente se daño, y no se le dio mantenimiento ya que el costo era muy elevado, y optaron por quitarlo.

La red del Gobierno Provincial de Tungurahua esta interconectado mediante cable UTP CAT 5e con el estándar EIA/TIA 565B también tiene conexión mediante fibra óptica que proporciona el internet e interconecta la red de los 2 edificios del H.G.P.T.

La red utilizada en el H.G.P.T es una solución segura y estable con calidad media para la conectividad a Internet, que permite gran movilidad dentro del alcance de la red.

Fuente: Observación **Elaborado por**: Daniel Portero

Observación Nº2

Protocolos de comunicación que se utiliza en la conexión con las bodegas

Tabla Nº 4.4 Protocolos de comunicación

Protocolos	Capa
TCP-UDP	Transporte
TCP-UDP 1001	Transporte

Fuente: Observación

Elaborado por: Daniel Portero

Los Protocolos que utilizan para la comunicación son TCP, UDP y TCP-UDP 1001 en la capa de transporte.

TCP-UDP con el cual establecen la comunicación mediante internet, con los cuales envían y reciben la información.

TCP-UDP 1001 permite recibir los datos que envía el reloj biométrico que se encuentra en las bodegas antiguas del H.G.P.T

Esto quiere decir que actualmente, únicamente utilizan conexión a internet y un reloj biométrico para comunicarse entre las bodegas y el departamento de sistemas del HGPT.

Fuente: Observación

Elaborado por: Daniel Portero

Observación Nº3

Eficiencia de la conexión que existe entre el edificio central y las bodegas del H.G.P.T

La eficiencia de la conexión o de la comunicación que existe entre el edificio del H.G.P.T. y las bodegas es media ya que el HGPT contaban con un radio enlace pero se daño a causa de un rayo, mediante este radio enlace se podía enviar la información con un ancho de banda alto en este caso era 10 Mbps.

Ahora el departamento de sistemas del H.G.P.T cuenta únicamente con una conexión remota y una conexión telefónica para la comunicación con las bodegas lo que significa que no hay mucha eficiencia para enviar y recibir información.

Fuente: Observación

Elaborado por: Daniel Portero

Observación Nº4

Nivel de seguridad de los sistemas de comunicación del departamento de sistemas del H.G.P.T para él envió y recepción de información

Tabla Nº 4.5 Seguridad en los Sistemas de comunicación

Servicio	Servidor	Plataforma Servidor
Firewall	Symantec Gateway Security	Linux
Internet Compartido	Squid 3.0	Solaris 10
Correo electrónico	Lotus Domino 7.01	Solaris 10
Antivirus	Symantec EndPoint Protection 11	Windows 2008 Enterprise
Controlador de Dominio	Active Directory	Windows 2008 Enterprise
DNS	DNS Server	Windows 2008 Enterprise
Adquisición de Materiales	Base datos documentales de Lotus Domino	Solaris 9
Sistema de Control de Recursos Humanos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema Médico Odontológico	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema de Control de Proveedores	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema Financiero FINANSG	Aplicación en Power Builder con base de datos de SQL 2005 Server	Windows 2008 Advanced Server

Fuente: Observación

Elaborado por: Daniel Portero

Tabla Nº 4.6 Seguridad mediante los servidores

No.	Nombre	Descripción	Sis. Operativo	Aplicaciones
1	HP PROLAINT	Servidor de Internet e Intranet	Ubuntu Server 9.04	Proxy Server - Squid 3.0 Stable 16 LAMP - Apache 2.2.11 - MySQL 5.0.75 - PHP 5.2.6-3Ubuntu4.1 Intranet - Joomla 1.5.14 Spanish
2	SunFire280r	Servidor de Correo Electrónico Interno	Solaris 9	Correo Electrónico Corporativo - Lotus Domino 8.0 Base de Datos Sistema Medico Odontológico - Oracle 9i
3	SunFireV440	Servidor de Bases de Datos	Solaris 10	Base de Datos Sistema de Control de Recursos Humanos (SCRH) - Oracle 10g Sistema de Control de Versiones (para cambios de la aplicación del SCRH, Visual Studio 2005) - Subversion 1.5 Base de Sistema para la Información, Seguimiento y evaluación de Proyectos - Postgress 8.4 - Jboss 5.0.1
4	Dominio (Tipo Blade)	Servidor de Dominio, DNS y Antivirus	Windows 2008 Server Enterprise	Controlador Principal de Dominio - Active Directory Servidor Primario de DNS Servidor de Actualizaciones - Windows Server Update Services 3.0 SP1 Antivirus Corporativo - Symantec EndPoint Protection 11 MR4
5	ServidorDF	Servidor de	Windows 2008	Respaldo del Controlador de

		Sistema Contable FINANSG	Advanced Server	Dominio - Active Directory Servidor de datos de los sistemas contables, rol de pagos, activos fijos, inventarios(FINANSG) - SQL SERVER 2005
6	ServidorHP	Servidor de Aplicación Mapeo de Actores	Linux Fedora 10	Sistema de Mapeo de Actores MySQL
7	GIS (Tipo Blade)	Servidor de Infosistema Geográfico	Centos 5.6	Sistema de Información Geográfica - Pmapper - Postgis(postgres)

Fuente: Observación
Elaborado por: Daniel Portero

El nivel de seguridad es bueno ya que en el H.G.P.T. posee un servidor especial para Firewall Symantec Security en plataforma Linux, el cual brinda los servicios de SPAM, IDS, Filtrado de Contenidos.
También posee un Servidor para antivirus corporativo Symantec EndPoint Protection 11 en plataforma Windows 2008 Enterprise.

ANALISIS GENERAL

El HGPT cuenta con diferentes departamentos los cuales comparten la información y recursos mediante la red interna, esta red cuenta con 165 dispositivos de red entre computadores, servidores, equipos inalámbricos, relojes biométricos y puntos de impresión en red, interconectado el edificio matriz y el centro de promociones y servicios de la provincia, con los principales servicios de red como: internet corporativo con restricciones de navegación (proxy), correo corporativo, automatización de procesos de solicitud de compras, seguridad de navegación, dominio de red para recursos compartidos y usuarios así como

también la utilización de antivirus corporativo.

Todos los servicios mencionados funcionan mediante los diferentes servidores que se encuentran en el departamento de sistemas los cuales ya analizados podemos concluir que tienen un desempeño medio, ya que poseen sistemas operativos un poco antiguos con lo que en un futuro podrían presentar problemas de seguridad y compatibilidad al desempeñar sus funciones.

Por lo que se tendría que actualizar los sistemas operativos para migrar a nuevas tecnologías, ya que los diferentes departamentos necesitan aplicaciones actuales para su correcto desempeño en el HGPT.

El mantenimiento periódico de los dispositivos de comunicación es algo fundamental ya que asi se mantendría un nivel de eficiencia lo suficientemente bueno para que la RED funcione correctamente.

El H. Gobierno Provincial de Tungurahua poseía un sistema de comunicación inalámbrico que comunicaba sus bodegas y talleres con su edifico Principal, el cual estaba interconectado mediante enlaces Spread Spectrum de 2.4GHz, el mismo que estaba legalmente registrado en la Secretaría Nacional de Telecomunicaciones, con su debido permiso de funcionamiento.

A causa de un problema desconocido el enlace Spread Spectrum sufrió un daño muy grave en uno de los sistemas, lo cual perjudico mucho al HGPT dejándolo casi incomunicado con sus talleres y bodegas, no se le dio mantenimiento ya que involucraba grandes gastos en su reparación, ese fue el motivo por el cual no existe un sistema de comunicación entre las bodegas y el edificio Principal del HGPT.

La única conexión que existe hoy en día entre las bodegas y Edificio del HGPT es un reloj Biométrico que controla la entrada y salida del personal que labora en esas localidades.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El problema que fue investigado en el siguiente proyecto se enfoca a la subutilización de la red existente en el H.G.P.T

- Los equipos utilizados en el departamento de sistemas del H.G.P.T utilizan plataformas o sistemas operativos desactualizados lo cual afecta en lo referente a compatibilidad con aplicaciones actuales o sistemas de comunicación.

- Es notorio que el H.G.P.T cuenta con un sistema de comunicación deficiente desde el departamento de sistemas hacia sus bodegas, ya que al no reparar su sistema de comunicación (radio enlace) la comunicación es de baja calidad, por que actualmente la realizan únicamente mediante el internet, sin ningún tipo de seguridad y mediante el teléfono convencional.

- El ancho de banda utilizado en el departamento de sistemas permite que el sistema de comunicación en este caso el internet funcione de una manera adecuada y permita enviar y recibir información.

5.2 RECOMENDACIONES

- Es necesario que a esta entidad se implemente un sistema que cumpla a cabalidad con todos los requerimientos necesarios para que así la información que se genere en las nuevas bodegas puedan ser controladas por los funcionarios del H.G.P.T.

- Se recomienda actualizar las plataformas de los servidores ya que así se mejoraría los protocolos de seguridad en los sistemas de comunicación.

- Es de vital importancia que se actualicen y se de mantenimiento a los sistemas operativos y a los equipos de comunicación cada determinado tiempo ya que de ellos depende el correcto funcionamiento de los procesos de comunicación del H.G.P.T

- Es de suma importancia tener el ancho de banda apropiado para abastecer las necesidades de una red que proveerá voz, datos, y posiblemente video ya que la herramienta de video será implementada a posterior para la vigilancia de las bodegas.

CAPÍTULO VI

PROPUESTA

6.1 DATOS INFORMATIVOS

Título:

"Diseño de una conexión VPN que permita mejorar el sistema de comunicación proporcionando la transmisión de información entre el H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas ubicadas en el sector de Catiglata."

Institución Ejecutora: H. GOBIERNO PROVINCIAL DE TUNGURAHUA

Tutor: Ing. Pilar Urrutia

Autor: Daniel Portero

Beneficiarios: Los principales favorecidos serán el personal del departamento de sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA

Ubicación: Provincia de Tungurahua, Cantón Ambato, Parroquia Catiglata

Equipo Técnico Responsable:

El desarrollo de la propuesta lo realizó el autor del presente trabajo investigativo Daniel Portero, conjuntamente con los miembros del departamento de sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA

6.2 Antecedentes de la Propuesta

Existen diferentes entidades como el H. GOBIERNO PROVINCIAL DE TUNGURAHUA que para satisfacer las necesidades de la empresa ha creado diferentes sucursales o bodegas en diferentes lugares tanto cerca de la empresa como en un lugar alejado, es por eso que se han visto en la obligación de centralizar su información a su edificio o localidad principal.

La migración de las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA ha provocado que los funcionarios pierdan comunicación con las instalaciones ubicadas en el sector de Catiglata, con lo cual no hay un control de la información y del personal y existe inseguridad en los equipos o maquinaria que aquí se almacena. Se ha propuesto generar una conexión desde el sector en el cual se encuentran actualmente las bodegas con un enlace inalámbrico pero no existe una línea directa de enlace. Motivo por el cual surge la necesidad de controlar el problema, con lo cual se plantea como solución el diseño de una conexión VPN.

En lo que respecta a los servicios a brindar, se determinó que la red se la utilizará para la transmisión de información voz y datos, los equipos de video serán implementados a posterior cuando ya las bodegas estén construidas totalmente.

6.3 Justificación

Recursos tecnológicos

El diseño de una conexión VPN permitió que se enlace el departamento de Sistemas del HGPT con sus bodegas en Catiglata, con lo cual se transmitió información de una manera segura por un canal confiable de comunicación a través de la red mundial que es el internet.
Con el uso de una VPN se garantiza la seguridad de la información, por ende una conexión segura.

Recursos humanos

El departamento de sistemas del HGPT cuenta con 3 Ingenieros en Sistemas y un Técnico en Electrónica, los cuales poseen los conocimientos necesarios para manipular y dar mantenimiento a la Conexión VPN.

Recursos económicos

En el desarrollo de esta investigación no hubo la necesidad de recursos económicos ya que los equipos utilizados existían en el departamento de Sistemas, y también porque proyecto se basa en software.

Infraestructura

Las bodegas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA cuentan con una red pequeña la cual esta conformada por un servidor Ubuntu 12.04, 3 Computadores HP Core 2 Quad y un Router D-Link 600, estos equipos sirvieron para establecer la conexión con el departamento de Sistemas del HGPT.

Información y Comunicaciones

Se cuenta con la información adecuada y la ayuda del personal del departamento de Sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA para el desarrollo de este proyecto, los resultados de esta investigación sobre Conexión VPN servirán de guía para que las empresas la consideren como una nueva alternativa en el momento de adquirir u optimizar sus conexiones remotas, proporcionando suficientes conocimientos acerca de una nueva forma de establecer redes de datos más económicas y seguras.

6.4 Objetivos

6.4.1 Objetivo General

Proponer la VPN como un medio de conexión entre el edificio del H. GOBIERNO PROVINCIAL DE TUNGURAHUA y sus bodegas ubicadas en sector de Catiglata.

6.4.2 Objetivo Específicos.-

- Identificar la configuración más adecuada para el establecimiento de la conexión VPN entre el edificio del H.G.P.T y sus bodegas en Catiglata.

- Utilizar Asterisk que es un software libre para dar el servicio de voz entre las bodegas y edificio del H.G.P.T

- Utilizar diferentes medios o aplicaciones para hacer mas entendible la configuración de la VPN

- Aplicar Open Vpn en Ubuntu 12.04 Server para establecer la VPN

- Crear un cliente remoto en Windows 7 para comprobar la comunicación entre el Servidor y el Cliente VPN mediante un pin y compartiendo archivos.

6.5 Análisis De Factibilidad

Factibilidad técnica:

La propuesta del diseño de una conexión VPN es factible debido a que existe los equipos necesarios y documentación respectiva para la implementación del sistema, además de varias alternativas que permitirán escoger la más apropiada y la que mejor se adapte a las necesidades de la empresa.

A continuación se detalla el Hardware y el software utilizados en el proyecto:

Hardware

- 2 Computadores Core 2Quad, Win7, 2.66Gz
- Laptop Toshiba Core 5, Win7

Software

- Sistema operativo Ubuntu 12.04
- Sistema Operativo Windows 7
- Asterisk 1.8.11-cert2
- Tunnelier 4.4
- Webmin 1.580
- OpenVpn 2.2.2
- X-Lite 5.0.0
- Wireshark 1.6.8

Factibilidad operativa: Desde el punto de vista operativo la propuesta es factible debido a que el H. Gobierno Provincial de Tungurahua, cuenta con la infraestructura tanto física como tecnológica requerida para la instalación de la red. Además la institución cuenta con personal calificado para la administración, control y mantenimiento de la conexión VPN, los mismos que podrán manejar cualquier problema que se presente en la red.

Factibilidad Económica: El administrador del departamento de sistemas del H.G.P.T consintió la creación de una conexión entre sus bodegas y su edificio matriz que permitirán la transmisión de información y otros servicios, que agilitaran y facilitaran el trabajo en esta institución, la ventaja de la realización del proyecto es que no hubo ningún gasto, ya que los equipos fueron tomados del departamento de sistemas de HGPT.

Factibilidad Bibliográfica: En lo referente a la documentación el proyecto es factible ya que existe información acerca de conexiones VPN de diferentes tipos, en documento, páginas web y revistas tecnológicas, aplicables a diferentes sistemas operativos.

Por lo tanto el presente proyecto es completamente factible de realizar

6.6 Fundamentación

6.6.1 VPN Basadas en SSL/TLS

Los protocolos SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de la capa de transporte que proporcionan comunicaciones seguras en Internet. SSL/TLS permite la autenticación tanto de cliente como servidor, usando claves públicas y certificados digitales y proporciona comunicación segura mediante el cifrado de la información entre emisor y receptor. SSL/TLS funciona por encima del protocolo de transporte (normalmente TCP) y por debajo de los protocolos de aplicación. Este protocolo está muy extendido para realizar actividades de comercio electrónico de tal manera que Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

Hay que destacar que SSL/TLS se compone de cuatro protocolos. Estos protocolos funcionan de manera idéntica en SSL y en TLS pero incorporan algunos detalles en TLS para su mejor funcionamiento. A continuación se definen estos cuatro protocolos sin entrar en mucho detalle:

- **Record Protocol:** Record Protocol encapsula los protocolos de nivel más alto y construye un canal de comunicaciones seguro. Se podría decir que es un protocolo de transporte.

- **Handshake Protocol:** Handshake Protocol se encarga de gestionar la negociación de los algoritmos de cifrado y la autenticación entre cliente y servidor. Define las claves de sesión utilizadas para cifrar. Se podría decir que es un protocolo de autenticación.
- **Change Cipher Spec Protocol:** Es un mensaje de un byte para notificar cambios en la estrategia de cifrado.
- **Alert Protocol**: Alert Protocol eñaliza alertas y errores en la sesión establecida.

Sin entrar en mucho detalle (más adelante en este mismo apartado se profundizará mas sobre el funcionamiento de SSL/TLS) SSL se basa en un esquema de clave pública para el intercambio de claves de sesión. En primer lugar cliente y servidor intercambian una clave de longitud suficiente mediante un algoritmo de cifrado asimétrico como RSA o Diffie-Hellman utilizando certificados. Mediante esa clave se establece un canal seguro, utilizando para ello un algoritmo simétrico previamente negociado. Los mensajes a ser transmitidos, se fragmentan en bloques, se comprimen y se les aplica un algoritmo Hash para obtener un resumen (MAC del mensaje) para asegurar la integridad asi como se muestra en el Grafico 6.1.

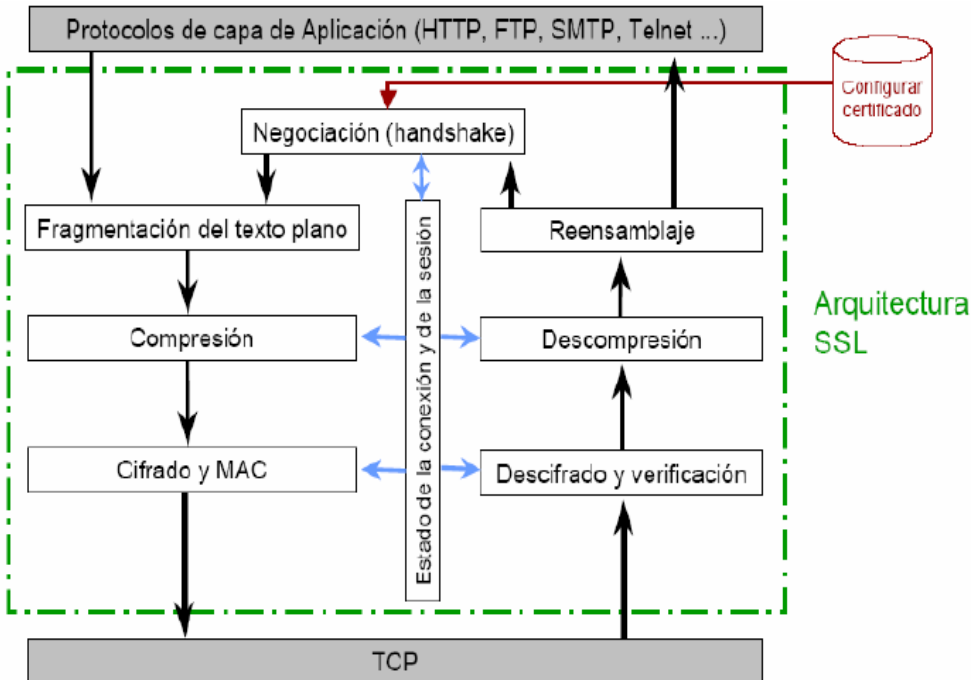


Gráfico Nº 6.1 Arquitectura SSL/TLS

FUENTE:http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

Para poder entender bien el funcionamiento de SSL/TLS se tendrá que definir los conceptos de sesión y conexión para estos protocolos.

En SSL/TLS una sesión es una asociación entre un cliente y un servidor. Las sesiones se crean mediante el protocolo Handshake y coordina los estados del cliente y del servidor. El estado de una sesión incluye la siguiente información:

- ✓ Identificador de Sesión: Consiste en una secuencia arbitraria de bytes elegida por el servidor para identificar una sesión activa.
- ✓ Certificado de la Entidad Par: Es el certificado del otro extremo de la comunicación (puede ser nulo).
- ✓ Método de Compresión: Indica el algoritmo usado para comprimir los datos antes de cifrarlos.
- ✓ Especificación de Cifrado: Especifica el algoritmo de cifrado de datos (DES, AES,...) y el algoritmo MAC (MD5 o SHA-1). También define atributos como el tamaño del Hash.
- ✓ Clave Maestra: Es una clave secreta de 48 bytes intercambiado entre cliente y servidor.

En SSL/TLS una conexión es transitoria y está asociada solamente a una sesión, mientras que una sesión puede tener múltiples conexiones. En otras palabras, las sesiones se usan para evitar la costosa negociación de los parámetros de cada conexión.
El estado de una conexión incluye la siguiente información:

- ✓ Valores Aleatorios del Servidor y del Cliente: Es una secuencia de bytes elegido por el servidor y el cliente para cada conexión
- ✓ Clave Secreta MAC de Escritura del Servidor: Es el secreto utilizado en operaciones MAC sobre los datos del servidor.
- ✓ Clave Secreta MAC de Escritura del Cliente: Es el secreto utilizado en operaciones MAC sobre los datos del cliente.

- ✓ Clave de Escritura del Servidor: Es la clave secreta para el cifrado de datos por el servidor y descifrado de datos por el cliente.
- ✓ Clave de Escritura del Cliente: Es la clave secreta para el cifrado de datos por el cliente y descifrado de datos por el servidor.
- ✓ Vector de Inicialización (IV) del Cliente y Servidor: Son vectores de inicialización utilizados para bloques de cifrado en estado CBC.
- ✓ Número de Secuencia: Cada estado de conexión contiene un número de secuencia que se mantiene independientemente para los estados de lectura y escritura. El número de secuencia debe ser reseteado a cero cada vez que un estado de conexión pasa a estado activo

Tras haber definido los conceptos de conexión y sesión en SSL/TLS se va a explicar el funcionamiento de SSL/TLS explicando, con más detalle, los cuatro protocolos de los que se compone SSL/TLS: Record Protocol, Handshake Protocol, Change Cipher Spec y Alert Protocol.

6.6.1.1 Record Protocol.

EL SSL/TLS Record Protocol es el protocolo de transporte que proporciona a cada conexión:

- **Confidencialidad:** Utilizando una clave compartida generada durante el protocolo Handshake para el cifrado convencional de los datos.
- **Integridad del Mensaje:** El protocolo de Handshake también genera una clave secreta común que se usa para formar el MAC o código de autenticación del mensaje.

En el funcionamiento del SSL Record Protocol intervienen mecanismos criptográficos, para los cuales son necesarios ciertos parámetros como la clave secreta para el cifrado.

Estos parámetros se negocian durante el establecimiento del protocolo Handshake, que además permite la autenticación de cliente y servidor.

El proceso que sigue el SSL/TLS Record Protocol es el siguiente:

1. Los mensajes se fragmentan en bloques de 214 bytes o menos.
2. Se aplica compresión opcionalmente.
3. Se calcula un MAC o una función Hash sobre los datos comprimidos.
4. El MAC junto con el mensaje se cifra con un algoritmo simétrico.
5. Finalmente se le añade una cabecera de registro o SSL Record Header

6.6.1.2 Handshake Protocol.

Mediante este protocolo se generan los parámetros criptográficos que van a definir el estado de una sesión (una sesión SSL/TLS siempre empieza con el Handshake). Este protocolo permite la autenticación entre el cliente y el servidor y la negociación de los algoritmos de cifrado y las claves y subclaves. Por ejemplo, uno de los parámetros a los que deben llegar a acuerdo el cliente y el servidor es la versión de SSL/TLS y método de compresión.

Este protocolo consta de cuatro fases en los que se negocian los parámetros de una sesión:

− Fase 1: Aquí se establecen las capacidades de seguridad (versión de protocolo, identificador de sesión, suite de cifrado, método de compresión y números aleatorios iniciales).
− Fase 2: En esta fase el servidor puede enviar un certificado, intercambio de clave y solicitud de certificado.
− Fase 3: El cliente envía su certificado, en caso de habérselo solicitado, el intercambio de clave y puede que envíe verificación de certificado.

− Fase 4: Se produce el intercambio de suite de cifrado y finalización del protocolo Handshake. En esta fase se completa el establecimiento de la conexión segura.[11]

6.6.1.3 Funcionamiento interno

Ahora unos conceptos que forman parte del funcionamiento interno de SSL/TLS

Cifrado

El cifrado es el proceso que transforma tu información de manera que no cualquier usuario pueda entenderla, se realiza con base a un elemento único conocido como llave, así nadie, excepto el poseedor puede leerla. El procedimiento inverso al cifrado es el descifrado.

Llave pública y llave privada

Son un par de "llaves" digitales asociadas a una persona o entidad y generadas mediante métodos criptográficos. La llave pública es usada para cifrar la información, haciendo una analogía, es como la llave utilizada para cerrar una puerta y mantener fuera a cualquier persona mientras que la llave privada se usa para descifrar, es decir, la llave que abre la puerta y sólo la posee la persona autorizada, por lo tanto ésta debe mantenerse en secreto.

Firma digital

Es un elemento que identifica y distingue a una persona de las demás y que al firmar con ella adquieres derechos y obligaciones. La firma digital se genera con base a la llave privada de quien firma y por lo tanto es única.

[11] http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

Certificado Digital SSL/TLS

Es un documento digital único que garantiza la vinculación entre una persona o entidad con su llave pública, esto se muestra en el Grafico 6.2

Contiene información de su propietario como nombre, dirección, correo electrónico, organización a la que pertenece y su llave pública, así como información propia del certificado por mencionar: periodo de validez, número de serie único, nombre de la AC que emitió, firma digital de la AC cifrada con su llave privada y otros datos más que indican cómo puede usarse ese certificado.

Microsoft Root Aut...	Microsoft Root Authority	31/12/2020	Microsoft Root A...
Microsoft Root Cert...	Microsoft Root Certifi...	09/05/2021	Microsoft Root C...
NO LIABILITY ACC...	NO LIABILITY ACCEP...	07/01/2004	VeriSign Time St...
Thawte Premium Se...	Thawte Premium Serv...	31/12/2020	thawte
thawte Primary Ro...	thawte Primary Root CA	16/07/2036	thawte
Thawte Server CA	Thawte Server CA	31/12/2020	thawte
Thawte Timestampi...	Thawte Timestamping...	31/12/2020	Thawte Timesta...
UTN-USERFirst-Obj...	UTN-USERFirst-Object	09/07/2019	USERTrust

Gráfico Nº 6.2 Certificados SSL/TLS

FUENTE:http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

HTTPS

Simplemente es una combinación del protocolo HTTP (usado en cada transacción web) con el protocolo SSL/TLS usada para establecer comunicaciones cifradas en sitios web.

Verificación de validez del certificado

Una vez que el navegador tiene el certificado del sitio web o de la aplicación, realiza algunas verificaciones antes de confiar en el sitio:

Integridad del certificado

Verifica que el certificado se encuentre íntegro, esto lo hace descifrando la firma digital incluida en él mediante la llave pública de la AC y comparándola con una firma del certificado generada en ese momento, si ambas son iguales entonces el certificado es válido.

Vigencia del certificado

Revisa el periodo de validez del certificado, es decir, la fecha de emisión y la fecha de expiración incluidos en él.

Verifica emisor del certificado

Hace uso de una lista de Certificados Raíz almacenados en tu computadora y que contienen las llaves públicas de las ACs conocidas y de confianza. Puedes acceder a esta lista desde las opciones avanzadas de tu navegador web (en este caso usamos Google Chrome).

Con base a esta lista, el navegador revisa que la AC del certificado sea de confianza, de no serlo, el navegador mostrará una advertencia indicando que el certificado fue emitido por una entidad en la cual no confía.

Estableciendo la conexión segura

Se estableció conexión una vez que el certificado cumplió con todas las pruebas del navegador, se establece la conexión segura, lo cual se traduce en seguridad para tus valiosos datos personales.[12]

[12] http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

6.6.1.4 Ventajas de SSL/TLS:

Las ventajas que ofrece el protocolo SSL/TLS son:

- Ofrece confidencialidad (cifrado simétrico), autenticación del servidor y del cliente (este último opcional) e integridad de los mensajes brindando unos niveles de seguridad excelentes que permiten el establecimiento de extranets con confianza y tranquilidad
- SSL constituye la solución de seguridad implantada en la mayoría de los servidores Web que ofrecen servicios de comercio electrónico ya que ofrece un canal seguro para el envío de números de tarjeta de crédito.
- Bajos costos de mantenimiento y no requiere mantenimiento en los clientes además de tener una buena interoperabilidad
- Se pueden encontrar en Internet numerosas implementaciones de libre distribución para implementar redes privadas virtuales basadas en SSL/TLS.[13]

6.6.2 OpenVPN

OpenVPN es una solución de conectividad basada en software, una utilidad de código abierto (está publicado bajo la licencia GPL, de software libre) para soluciones SSL/TLS VPN. La facilidad de uso de OpenVPN ha simplificado mucho la configuración de las VPN y arroja a la basura muchas de las complejidades que caracterizan a otras implementaciones de VPN, como por ejemplo, la que más se va a mencionar por su importancia e influencia en el mercado, IPSec, y ha hecho más accesible para la gente inexperta este tipo de tecnología. El modelo de seguridad de OpenVPN está basado en la arquitectura SSL/TLS, que es el estándar escogido actualmente por la industria para establecer comunicaciones seguras a través de Internet.

[13] http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

Un aspecto que hay que tener en cuenta durante todo el estudio con OpenVPN es que esta herramienta implementa redes seguras en la capa 2 o 3 (según el modo que utilice OpenVPN: Tunnel o Bridge) de la pila de protocolos OSI utilizando como extensión el protocolo SSL/TLS, soportando métodos de autenticación del cliente de manera flexible. Las implementaciones de SSL/TLS más conocidas hoy en día operan a través de un navegador Web (lo que se conoce como HTTPS), ya que se han implementado aproximaciones de SSL/TLS para aplicaciones en la capa de aplicación de la pila OSI (capa 7). Pero hay que tener muy en cuenta que este tipo de implementación Web con SSL/TLS no es una VPN y que OpenVPN no es una aplicación Web Proxy ni opera a través de un navegador Web, ya que opera sobre la capa 2 o 3 de la pila OSI. Por tanto, un cliente de

OpenVPN no podrá utilizar un navegador Web para conectarse al servidor de OpenVPN y mantener una comunicación segura a través de la VPN.

Otra de las ventajas de utilizar OpenVPN es la compatibilidad que ofrece con la infraestructura de clave pública (PKI) mediante el uso de certificados X.509 y la técnica de intercambio de claves RSA, compatible con NAT, DHCP y con los dispositivos de red virtuales TUN/TAP. Por el contrario, OpenVPN no ofrece compatibilidad con estándares tales como IPSec, IKE, PPTP o L2TP.
La razón por la que OpenVPN utiliza este protocolo, es porque TLS es la última evolución de la familia de protocolos SSL desarrollados en un principio, en 1996, por Netscape para asegurar el primer navegador Web de dicha firma. TLS y las versiones antiguas y actuales de SSL han visto generalizado el uso de la Web durante muchos años y han sido ampliamente analizados por las deficiencias que tenían en estas implementaciones. A su vez, este análisis ha dado lugar a un consecuente fortalecimiento del protocolo de tal manera que hoy, el protocolo SSL/TLS se considera uno de los más fuertes y más maduros protocolos seguros disponibles. Por estos motivos y por otros tantos, TLS es una excelente elección para implementar los mecanismos de autenticación y mecanismos de intercambio de claves en una VPN.

OpenVPN no opera en el kernel, sino que opera en el espacio de usuario incrementando de esta manera la seguridad y la escalabilidad. Según el autor, James Yonan, uno de los mayores frenos de IPSec es que añade una gran complejidad en kernel. Como ya se ha comentado la complejidad es el enemigo de la seguridad. El problema de añadir dicha complejidad de seguridad software en el kernel es que se ignora un importante principio de los sistemas de seguridad: nunca se ha de diseñar un sistema en el que si uno de los componentes cae pueda poner en peligro todo el sistema.

Un simple desbordamiento de un buffer en el espacio del kernel provocaría un compromiso total en la seguridad del sistema. Es por esta razón que OpenVPN ubica su complejidad y ejecuta su código dentro del espacio de usuario pudiendo contener los fallos en este espacio más rápidamente sin comprometer la seguridad del sistema.[14]

OpenVPN soporta diferentes medios de autenticación como certificados, smart cards, y/o usuarios/contraseñas, y permite políticas de control de acceso para usuarios o grupos usando reglas de firewall aplicadas a las interfaces virtuales de la VPN.

OpenVPN permite conectar múltiples clientes a un solo servidor OpenVPN sobre un simple puerto TCP o UDP.

.

6.6.2.1 Formas de trabajo del OpenVPN

Openvpn se puede dividir según su forma de trabajo en 3 tipos:

1) **Host a Host**: Es el método más simple, nos permite encriptar la comunicación entre dos PC las cuales deberán solamente tener conexión; es decir: ambas PC deben poderse enviar paquetes directamente ya sea

[14] http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

porque estén conectadas en la misma red local, o porque ambas estén conectadas a la internet y sean alcanzables entre sí.

2) **Road Warrior**: Es una de las formas más utilizadas y solicitadas por los estudiantes. Es el permitir que una máquina de alguien que esté fuera de nuestra red (de forma temporal o permanente) pueda comunicarse con el servidor OpenVPN de nuestra red y una vez autenticado pueda entrar a ver y acceder los recursos de nuestra red local. En verdad es un caso especial de la conexión Red a Red que a continuación mencionamos:

3) **Red a Red:** Uno de los métodos más usados. Mediante ésta forma dos redes separadas en el espacio pueden comunicarse como si estuvieran unidas por un cable virtual (de ahí la V de VPN); la comunicación entre ambas redes viajará encriptada una vez salgan de los servidores de Openvpn y hasta que lleguen a su otro extremo.

6.6.2.2 Ventajas del uso de OpenVPN

OpenVPN es un sistema de creación y uso de Vpn muy modesto y fácil de utilizar que nos permite implementar Vpn que de otras formas sería muy molesto o dificultoso de realizar.

Las implementaciones IPSec, aunque supuestamente mejor elaboradas y soportadas por el kernel de Linux, son muy difíciles de implementar en máquinas con Windows. En el caso de OpenVPN existen clientes y servidores tanto para Linux como para Windows y su implementación para redes o sistemas multiplataforma es muy sencilla de llevar a cabo.[15]

[15] http://www.ecualug.org/2007/02/06/comos/centos/c_mo_instalar_y_configurar_openvpn

6.6.2.3 Modo de Funcionamiento de OpenVPN

OpenVPN puede trabajar en dos modos: modo “tun” (o modo Tunnel) o modo “tap” (o modo Bridge). Ambos modos utilizan el adaptador TUN/TAP en concreto, utilizando el adaptador TUN para transmitir trafico IP a lo largo del túnel o, por el contrario, utilizando el adaptador TAP para transmitir tráfico Ethernet por el túnel. Como sabemos, la configuración de estos adaptadores es muy fácil y solo requiere de un conjunto de comandos o de líneas introducidas en un fichero de configuración. Una vez la interfaz TUN/TAP se ha establecido ya se puede hacer una comunicación mediante OpenVPN.

La principal diferencia entre los adaptadores tun y los adaptadores Tap es que un adaptador tun es como un dispositivo virtual IP punto a punto entre los dos extremos de la comunicación (como si de una línea dedicada entre los dos extremos de la comunicación se tratase) y un dispositivo Tap es como un dispositivo Ethernet virtual entre los dos extremos de la comunicación (como si se estableciese una red Ethernet los dos dispositivos de la comunicación).

Lo más normal es utilizar el modo tun para establecer un túnel IP entre ambos extremos de la comunicación, pero la gente que ejecuta aplicaciones que necesitan características típicas que puede ofrecer Ethernet (que no trabajan en una red exclusivamente IP) necesitarán entonces realizar un puente entre una red local física Ethernet mediante la utilización de un dispositivo tap virtual proporcionado por OpenVPN. Para ello se necesita un dispositivo tap en cada extremo de la comunicación. De esta manera OpenVPN permite encaminar trafico Ethernet broadcast y tráfico no IP como Windows NetBios o IPX a través de la VPN establecida mediante los adaptadores. En caso de no necesitar ninguna característica especial de Ethernet lo más usual es utilizar el modo tun mediante los dispositivos virtuales tun de OpenVPN, además es el procedimiento más utilizado por los usuarios por su facilidad de configuración.

6.6.2.4 Asignación de Direcciones

El direccionamiento IP utilizado típicamente para las redes privadas, como puede ser cualquier VPN particular implementada con OpenVPN. Para ello hay que decir que la IANA ha reservado los siguientes espacios de direcciones IP para las redes privadas como se muestra en el Grafico 6.3 (definida en el RFC 1918):

Grupo A	10.0.0.0	10.255.255.255	10/8
Grupo B	172.16.0.0	172.31.255.255	172.16/12
Grupo C	192.168.0.0	192.168.255.255	192.168/16

Gráfico Nº 6.3 Rango de direcciones para VPN

FUENTE:http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873

Estos bloques de direcciones IP son normalmente utilizados en las configuraciones de las VPN, pero es importante seleccionar las direcciones que minimizan la probabilidad de que haya un conflicto con las direcciones IP de red o de subred.

6.6.2.5 UDP y TCP

OpenVPN permite, la posibilidad de utilizar los protocolos TCP o UDP como protocolos de transporte para establecer la comunicación con el host remoto.

Para poder manejar esta característica OpenVPN proporciona la directiva --proto p donde p puede tener los valores Udp, Tcp-Client o Tcp-Server. El protocolo por defecto es udp, por tanto, OpenVPN utilizará el protocolo udp cuando la directiva --proto no sea utilizada. También se puede especificar que se quiere utilizar el protocolo udp especificando, para ello, la línea --proto udp. Para operar con el protocolo TCP, uno de los extremos (el servidor) debe incluir la línea --proto tcp-server y en el otro extremo (los clientes) se debe incluir la línea --proto tcp-client.

El extremo que incluye la directiva explicada con el valor tcp-server esperará indefinidamente la llegada de una petición de conexión. El extremo que incluye la directiva con el valor tcp-client hará el intento de conectarse al otro extremo, esperará, y si dicho intento falla, se quedará "dormido" durante 5 segundos (ajustable mediante la directiva --connect-retry, que tiene el valor por defecto de 5 segundos) e intentará conectarse de nuevo.

TCP optimiza el tamaño del paquete de manera que no sea necesario fragmentar el paquete durante su tránsito por Internet. El problema surge cuando se encapsula TCP sobre TCP, obteniendo un paquete más largo ya que ahora tenemos un paquete TCP, con un tamaño máximo de paquete, encapsulado dentro de otro paquete TCP, por lo que, intrínsecamente, será de mayor tamaño. Por tanto, esto provocará problemas de fragmentación que pueden ser graves en el sentido en que todos los paquetes chocarán con el primer Router que no sea capaz de encaminar paquetes demasiado grandes. Este problema, en Internet, se resume en que el host destino nunca podrá reensamblar el mensaje completo. Por tanto, de repente nos encontramos con el doble de paquetes, el doble de posibilidades de perder y retransmitir un paquete y el doble de paquetes que llegan y deben ser reensamblados.

OpenVPN ha sido diseñado originalmente para operar de manera óptima utilizando como protocolo de transporte UDP, pero TCP puede utilizarse en situaciones donde UDP no puede ser usado. En comparación con UDP, TCP es menos eficiente y menos robusto cuando es utilizado sobre redes que utilizan alguna capa fiable y con posibles congestiones. Existen algunos casos, sin embargo, donde utilizar TCP puede tener ventajas de seguridad y robustez frente a la utilización de UDP, como en el caso de utilizar túneles no IP o de utilizar aplicaciones sobre protocolos que no tienen ningún nivel de fiabilidad. Otro aspecto a favor de la utilización de UDP frente a TCP es que la utilización de UDP frente a TCP proporciona mejor protección frente a ataques de denegación de servicio (DoS) y frente al escaneo de puertos.

En muchas aplicaciones que se pueden utilizar sobre OpenVPN, como pueden ser los sistemas de VoIP, también conviene utilizar el protocolo UDP frente al protocolo TCP por diversas razones. Para empezar, en la mayoría de los casos, los sistemas VoIP utilizan el protocolo RTP (Real-time Transport Protocol) que es transportado utilizando el protocolo UDP. Como ya se ha comentado TCP proporciona una conexión fiable, pero este aspecto, en los sistemas VoIP no es bueno. Si utilizamos TCP en VoIP, cuando un paquete es rechazado, el emisor vuelve a retransmitir el paquete ante la petición del receptor o receptores. Pero en este caso al reensamblar los paquetes de voz retransmitidos en un stream de audio podrían resultar demasiado tarde para obtener una reproducción fiable del sonido original. Por el contrario, UDP da por bueno paquetes enviados fuera de orden y no existe verificación (ACK) de si el paquete llega. [16]

6.6.3 Asterisk

Asterisk es un software PBX que usa el concepto de software libre (GPL).
Digium, empresa que promueve el Asterisk, invierte en ambos aspectos, el desenvolvimiento de código fuente y en hardware de telefonía de bajo costo que funciona con Asterisk. El Asterisk corre en plataforma Linux y otras plataformas Unix con o sin hardware conectando a la red pública de telefonía, PSTN (Public Service Telephony Network).

El Asterisk permite conectividad en tiempo real entre las redes PSTN y redes Voip. Con Asterisk, usted no tiene apenas un cambio excepcional de su PBX. El Asterisk es mucho más que un PBX central. Con Asterisk en su red, Usted puede crear cosas nuevas en telefonía como:

- ✓ Conectar empleados trabajando desde casa para un PBX de la oficina sobre conexiones de banda ancha.
- ✓ Conectar oficinas en varias provincias sobre IP. Esto puede ser hecho por Internet o por una red IP privada.

[16] http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

- ✓ Dar a los funcionarios, buzón de voz, integrándolo con una "web" y sus e-mail.
- ✓ Construir aplicaciones de respuesta automática por voz, que puede conectarlo a un sistema de pedidos, por ejemplo, o a otras aplicaciones internas.
- ✓ Dar acceso al PBX de la compañía para usuarios que viajan, conectando sobre la VPN de un aeropuerto o un hotel.
- ✓ Y mucho más...

Asterisk incluye muchos recursos que solo eran encontrados en sistemas de mensajería unificada "sistema encima de la línea" como:

- Música en espera para clientes en filas de espera, soportando streaming de media así como música en MP3.
- Filas de llamada donde agentes de forma conjunta atienden las llamadas y monitorean dicha fila.
- Integración para sintetización de la conversación (text-tospeech).
- Registro detallado de llamadas (call-detail-records) para integración con sistemas de tarificación.

- Integración con reconocimiento de voz (Tal como el software de código abierto para reconocimiento de voz).
- La habilidad de interfaces con líneas telefónicas normales, ISDN en acceso básico (2B+D) y primario (30B+D).

6.6.3.1 Reducción extrema de costos

Si usted compara un PBX tradicional con Asterisk tal vez la diferencia sea pequeña, principalmente por los costos de hardware y los teléfonos IP.
Entretanto, Asterisk solo puede ser comparado a un PBX digital.
Comparar una central analógica de cuatro líneas FXO y 16 ramales con

Asterisk es injusto.

Cuando usted agrega recursos avanzados como Voz sobre IP, URA e DAC, la diferencia de costo es menor, en diversas oportunidades. Para dar un ejemplo, una única puerta de URA hoy con acceso a un mainframe, cotizada recientemente para un cliente nuestro, costó por lo menos 10 veces el precio que costaría con Asterisk.

6.6.3.2 Arquitectura Básica de Asterisk

Como puede ser visto en el Grafico 6.4, las tecnologías y protocolos de voz sobre IP son tratados como canales de Asterisk. Asterisk puede usar simultáneamente protocolos de tipo TDM, como el ISDN y interfaces analógicas, FXS y FXO, conjuntamente con canales VoIP en los estándares SIP, H323, MGCP, IAX e SCCP.

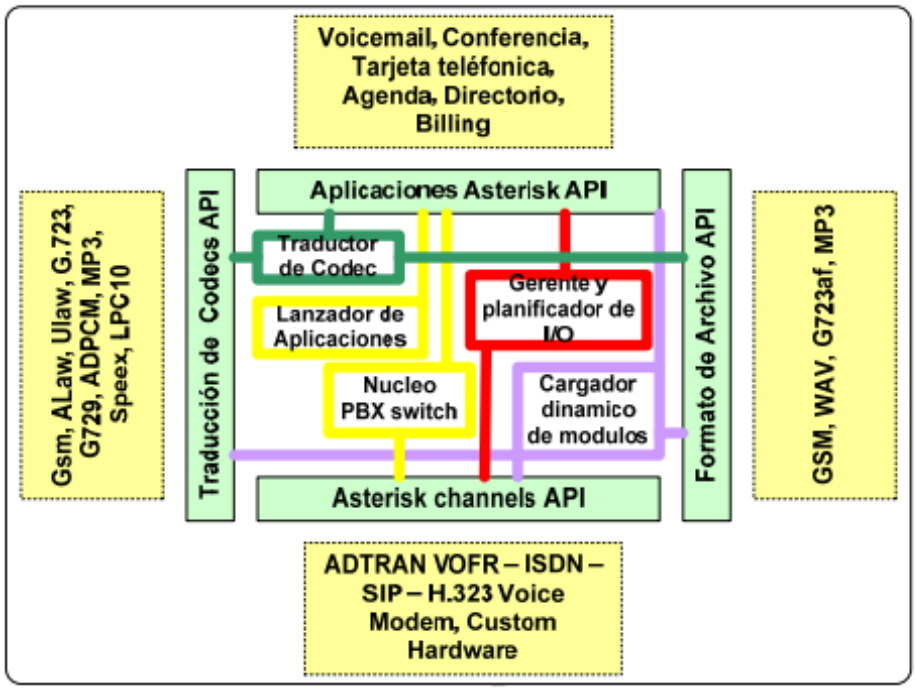


Gráfico Nº 6.4 Arquitectura de Asterisk

FUENTE: http://linux.ctt-espe.edu.ec/12.pdf

El punto fundamental de la arquitectura de Asterisk es que esta funciona como un Gateway de media entre todos estos protocolos y no solamente como un Proxy de señalización. Con esto, un canal puede estar configurado en IAX2 con codec GSM y se puede comunicar con otro canal configurado con SIP y Codec G.711.

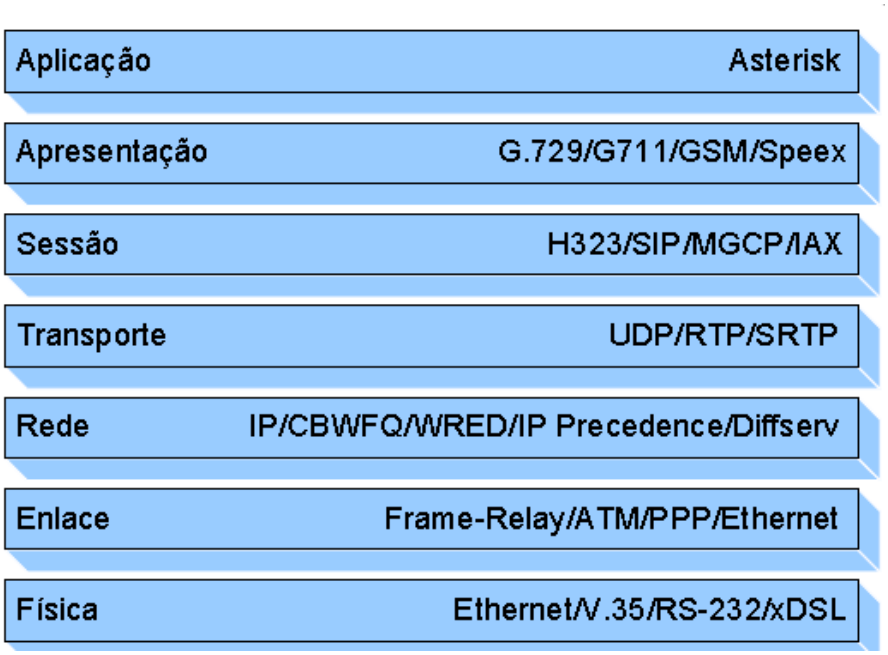


Gráfico Nº 6.5 Asterisk en la capa del modelo OSI
FUENTE: http://linux.ctt-espe.edu.ec/12.pdf

Como se puede ver en el Grafico 6.5, la voz sobre IP esta compuesto de diversos protocolos envolviendo varias capas del modelo OSI. De cualquier forma, VoIP es en verdad una aplicación que funciona sobre las redes IP actuales. Estaremos aquí tratando principalmente las capas de transporte, sesión, presentación y aplicación.

En la capa de transporte, la mayor parte de estos protocolos usa el RTP/RTCP, siendo el primero un protocolo de media y el segundo un protocolo de control. La excepción es IAX, que implementa un transporte de medio propio. Todos ellos usan UDP para transportar la voz.

En la capa de sesión entran los protocolos de voz sobre ip propiamente dichos, H323, SIP, MGCP, IAX e SCCP.

En la capa de sesión los CODECs definen el formato de presentación de voz con sus diferentes variaciones de compresión.

6.6.3.2.1 Canales

Un canal es el equivalente a una línea telefónica en la forma de un circuito de voz digital. Este generalmente consiste de una señal analógica en un sistema POTS o alguna combinación de CODEC y protocolos de señalización (GSM con SIP, Ulaw con IAX). En un principio las conexiones de telefonía eran siempre analógicas y por eso, más susceptibles a ruidos y ecos. Más recientemente, buena parte de la telefonía paso para el sistema digital, donde la señal analógica es codificada en forma digital usando normalmente PCM (Pulse Code Modulation). Esto permite que un canal de voz sea codificado en 64 Kilobits/segundo sin ser compactado.

Canales para voz sobre IP

Los canales para Voz sobre IP son:

- ✓ **chan_sip**: Session Initiation Protocol.
- ✓ **chan_iax:** Inter-Asterisk Exchange Protocol 2.
- ✓ **chan_h323**: ITU H.323
- ✓ **chan_mgcp**: IETF MGCP.
- ✓ **chan_sccp:** Cisco SCCP

Canales internos para Asterisk

Los canales internos para Asterisk son:

- ✓ **chan_agent:** Un canal de agente DAC. Dial String (Agent/agentnumber)
- ✓ **chan_console: Console:** Cliente de consola de Linux, driver para placas de sonido (OSS o ALSA). Dial string: console/dsp;
- ✓ **chan_local**: Pseudo canal. Hace un "loop" en el plan de discado. Dial **string**: Local/extension@context

6.6.3.3 Codecs y Conversores de CODEC

Los Codecs como se muestra en el Grafico 6.6 son usados para convertir una señal analógica de voz en una versión codificada digitalmente. Los Codecs varían en calidad de sonido, banda ancha necesaria y requisitos computacionales. Cada servicio, programa, teléfono o gateway, típicamente, soporta varios codecs diferentes y cuando van a hablar uno con otro, negocian que codec es el que van a usar. Algunos codecs como el G.729 necesitan de pagos de royalties para su uso.

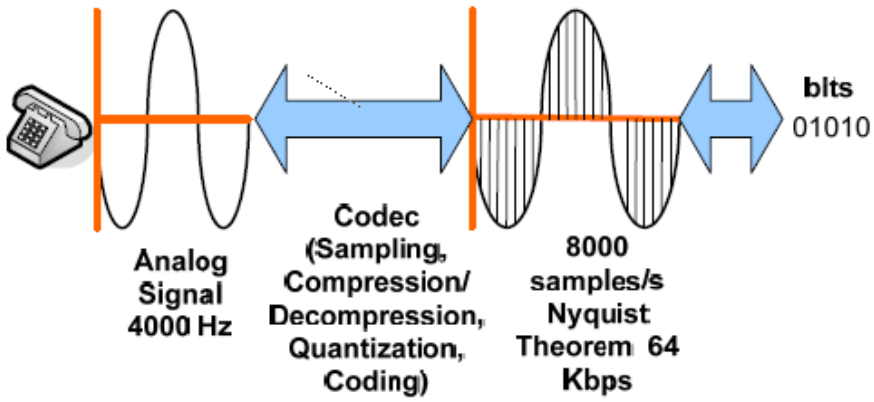


Gráfico Nº 6.6 Proceso de digitalización de VOZ
FUENTE: http://linux.ctt-espe.edu.ec/12.pdf

Obviamente es deseado colocar tantas llamadas cuanto sea posible en una red de datos. Esto puede ser hecho codificando en una forma que use menos banda ancha. Este es el papel de CODEC (COder/DECoder), algunos CODECs como el g.729 permite codificar a 8 Kilobits por segundo, una compresión de 8 para 1. Otros ejemplos son ulaw, alaw, gsm, ilbc y g729.
Asterisk soporta los siguientes CODECs:

- G.711 ulaw (usado en EUA) – (64 Kbps).
- G.711 alaw (usado en Europa y Brasil) – (64 Kbps).
- G.723.1 – Modo Pass-through
- G.726 - 32kbps en Asterisk1.0.3, 16/24/32/40kbps
- G.729 – Precisa adquisición de licencia, a menos que este siendo usando en modo pass-thru.(8Kbps)
- GSM – (12-13 Kbps)
- iLBC – (15 Kbps)
- LPC10 - (2.5 Kbps)
- Speex - (2.15-44.2 Kbps)[17]

6.6.3.4 Recomendaciones de la ITU para VOIP

Los tres códec más usados para transmitir Voz sobre IP son:

RECOMENDACIÓN G.711 G.711 utiliza una gran cantidad de ancho de banda para la transmisión, aunque tiene una puntuación MOS21
Esta recomendación de la ITU-T describe el algoritmo para el codificado de voz a 8 Kbps. Este códec tiene una puntuación MOS de 4,0, y es el códec utilizado

RECOMENDACIÓN G.723 Esta recomendación ITU-T describe un algoritmo de bajo ratio de compresión. Es un códec particularmente adecuado para transmisiones de voz sobre IP en entornos WAN de bajo ancho de banda, aunque tiene una baja puntuación MOS de 3,9.

[17] http://linux.ctt-espe.edu.ec/12.pdf

RECOMENDACIÓN G.729 Esta recomendación de la ITU-T describe el algoritmo para el codificado de voz a 8 Kbps. Este códec tiene una puntuación MOS de 4,0, y es el códec utilizado normalmente para instalaciones de Voz sobre IP. Este debido a que ofrece una alta compresión mientras mantiene una buena calidad de voz.[18]

6.6.3.5 Protocolos

Enviar datos de un teléfono a otro sería fácil si los datos encontrasen su propio camino para el otro teléfono destino. Desafortunadamente esto no sucede así, es preciso un protocolo de señalización para establecer las conexiones, determinar el punto de destino, y también cuestiones relacionadas a señalización de telefonía como el tono y tiempo de campanilla, identificador da llamada, desconexión etc. Hoy es común el uso de SIP (Session Initiated Protocol), muy usado hoy, y otros protocolos también muy en auge en el mercado como lo es el H.323, el MGCP y más recientemente el IAX que es excepcional cuando se trata de trunking y NAT (Network Address Translation). Asterisk soporta:

- SIP
- H323
- IAXv1 y v2
- MGCP
- SCCP (Cisco Skinny)[19]

6.6.3.6 Como escoger un protocolo

La elección de un Protocolo depende de ciertos factores que son muy importantes al momento de realizar una llamada, algunos de los factores son:

[18] http://www. repo.uta.edu.ec/handle/123456789/79
[19] http://linux.ctt-espe.edu.ec/12.pdf

- Ancho de banda
- Puertos por los que viajan a través de internet
- Compatibilidad con Teléfonos IP

6.6.3.6.1 SIP

Estándar abierto descrito por la IETF, largamente implementado, las principales operadoras VoIP están usando SIP. Es el protocolo estándar por defecto para la telefonía IP hasta el momento. Los puntos fuertes son: estándar de IETF, adopción en el mercado. Los puntos flacos son: problemas de uso de NAT, y que el uso de ancho de banda con RTP es alto.[20]

Los clientes SIP usan el puerto 5060 en TCP (Transmisión Control Protocolo de control de transmisión) y UDP (Protocolo Datagrama de Usuario) para conectar con los servidores SIP.

SIP es usado simplemente para iniciar y terminar llamadas de voz y video. Todas las comunicaciones de voz/video van sobre RTP (Protocolo de transporte en tiempo real).

Los protocolos más utilizados de esta arquitectura son:

- **RTP Y RTCP**: Utilizado principalmente para la entrega en tiempo real de los datos.

- **RTSP** (El protocolo de Flujo en tiempo Real): se utiliza para entrega bajo demanda de datos en tiempo real.

- **SDP** (Protocolo de Descripción de Sesión): Proporciona un formato estándar para el intercambio de capacidad de los medios.

[20] http://linux.ctt-espe.edu.ec/12.pdf

COMPONENTES DEL SISTEMA SIP

Gráfico Nº 6.7 Componentes de un sistema SIP
FUENTE: http://www. repo.uta.edu.ec/handle/123456789/79

- **Agentes de Usuario**: Aplicaciones de estaciones finales que envían y reciben peticiones SIP para beneficio de los usuarios.

- **Servidores Proxy**: Hace las veces de Gatekeeper en H.323.

- **Registradores:** Aceptan registros de usuarios que indican las direcciones en las que se las puede localizar. [21]

6.6.3.6.2 IAX

Protocolo abierto de Asterisk todavía no ratificado como una RFC. El IAX es eficiente en ancho de banda, su modo conocido como "trunked" permite que este use una única cabecera para el pasaje de varias llamadas. Otro punto fuerte de

[21] http://www. repo.uta.edu.ec/handle/123456789/79

IAX es el hecho de usar apenas el puerto UDP 4569 para señalización y audio. Con esto se torna simple la configuración de los Firewalls y de NAT.

6.6.3.6.3 MGPC

Es un protocolo para ser usado en conjunto con el H323, SIP y IAX. Su gran ventaja es la escalabilidad. Toda la inteligencia es implementada en los Call Agent contrarrestando a los gateways. Simplifica mucho la configuración. Puntos fuertes: manejo centralizado, puntos flacos, el protocolo es poco adoptado todavía.

6.6.3.6.4 H323

Muy usado en voz sobre ip. Esencial en la conectividad con proyectos más antiguos usando ruteadores Cisco o gateways de voz. H323 todavía es estándar para proveedores de PBX y ruteadores, hoy ellos comienzan a adoptar el SIP. Excelente para videoconferencia. Puntos fuertes, larga adopción en el mercado, estandarización por la ITU. Puntos flacos: complejo, poco adoptado en telefonía IP.[22]

El protocolo H.323 comprende a su vez una serie de servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF), estos se detallan en el siguiente Grafico 6.8

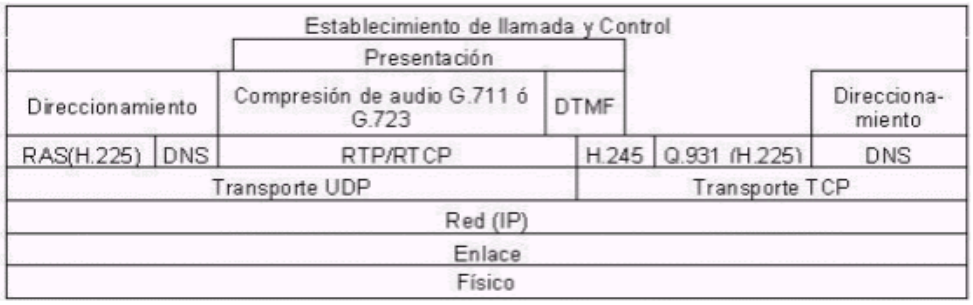


Gráfico Nº 6.8 Stack de protocolos H.323

FUENTE: http://www.monografias.com/trabajos11/descripip/descripip.shtml

[22] http://linux.ctt-espe.edu.ec/12.pdf

A. DIRECCIONAMIENTO

El direccionamiento según H.323 es:

- **Ras (Registro, Admisión and Estado):** Es un protocolo de comunicaciones que permite a una estación H.323 situar otra estación H.323 a través de un Gatekeeper.
- **DNS (Servidor de Dominio de Nombres).** Es un servicio de identificación de nombres en direcciones IP, idéntico al protocolo RAS pero a través de un servidor DNS.

B. SEÑALIZACIÓN

La señalización en H. 323 es:

- **Q.931**: Señalización inicial de llamada.
- **H.225**: Control de llamada: señalización, registro, admisión, y paquetización / sincronización del flujo de voz.
- **H.245**: Protocolo de control para especificar mensaje de apertura y cierre de canales para flujos de voz.

C. COMPRESIÓN DE VOZ

La compresión de Voz es:

- Requeridos: G.711 y G.723
- Opcionales G.728, G.729 y G.722

D. TRANSMISIÓN DE VOZ

La transmisión de Voz se da por los protocolos:

- UDP (Protocolo Datagrama de Usuario): La transición se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad de los datos, el aprovechamiento del ancho de banda es mayor en comparación con el protocolo TCP.

- RTP (Protocolo en Tiempo Real): Maneja los mecanismos de temporización, sincronización de diferentes flujos de tráfico marcando los

paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

E. CONTROL DE TRANSMISIÓN

El control de transmisión se da por:

- RTCP (Protocolo de Control en Tiempo Real): Es una función de control que se utiliza para detectar situaciones de congestión en la red y tomar acciones correctivas cuando sea necesario. [23]

6.6.3.7 Concepto de Peers, Users y Friends

Existen tres tipos de clientes SIP y IAX como se ve en el Grafico 6.9. El primero es el user. Los Usuarios pueden hacer llamadas a través de un servidor Asterisk, pero no pueden recibir llamadas del servidor. Esto es útil en una situación donde el usuario puede proveer algunos servicios telefónicos al cliente, pero nunca debe poder llamar a ciertos teléfonos, tal como es el caso para un proveedor de larga distancia. El segundo es el peer. Un peer es un cliente para el cual el usuario puede pasar las llamadas, pero que el usuario nunca va a recibir llamadas de este.

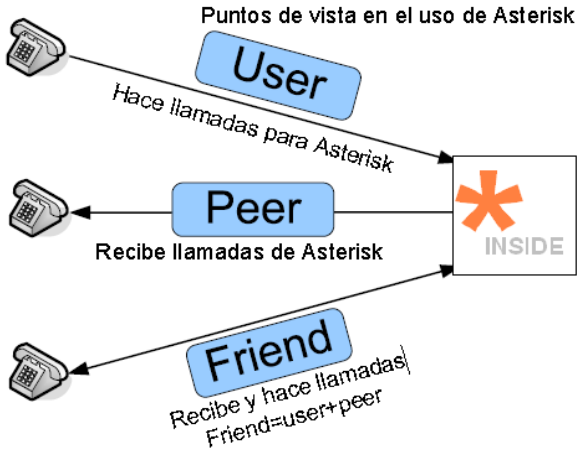


Gráfico Nº 6.9 Users, Peers y Friends
FUENTE: http://linux.ctt-espe.edu.ec/12.pdf

[23] http://www.monografias.com/trabajos11/descripip/descripip.shtml

Esto puede ser útil para tener un teléfono que solo reciba llamadas, o pasar llamadas a un servidor Asterisk de uso especial como por ejemplo un buzón de voz.24

6.6.4 Samba

Samba es un software que permite a un ordenador con Ubuntu poder compartir archivos e impresoras con otras computadoras en una misma red local. Utiliza para ello un protocolo conocido como SMB/CIFS compatible con sistemas operativos UNIX o Linux , como Ubuntu, pero además con sistemas Windows (XP, NT, 98...), OS/2 o incluso DOS. También se puede conocer como LanManager o NetBIOS[25]

6.7 Metodología

En lo que se refiere al diseño del proyecto, en primer lugar se realizó un análisis de las necesidades que surgieron en el HGPT, esto ayudo a determinar que se debía tomar en cuenta para el desarrollo del proyecto

Con esta información se inicio el proceso de diseño de la conexión, que sistema es el más indicado para que cumpla con la necesidad de dar comunicación a diferentes usuarios de esta entidad.

También se tomo en cuenta que los usuarios pueden aumentar, es por eso que se escogió ese tipo de configuración, con la cual se da una comunicación segura y efectiva.

[24] http://linux.ctt-espe.edu.ec/12.pdf
[25] http://www.guia-ubuntu.org/index.php?title=Samba

Se utilizo protocolo SSH lo cual sirvió para realizar la configuración del servidor desde un sitio remoto, esto nos facilito mucho el trabajo de ir a cada momento a las bodegas donde se encuentra el servidor.

Además, se incorporo un sistema de VOIP con la cual se dará comunicación por voz a la red que se encuentra en las bodegas del HGPT con los usuarios que se vayan incorporando en el servidor VPN.

6.8 Modelo Operativo

Una vez determinada la solución para las necesidades del HGPT, hemos determinado que para resolver los requerimientos tenemos que implementar el servidor VPN en las bodegas ubicadas en el sector de Catiglata ya que asi podremos tener acceso a la red LAN de la misma desde un cliente remoto.

RECOPILACIÓN DE INFORMACIÓN

H. GOBIERNO PROVINCIAL DE TUNGURAHUA

Su estructura organizacional se divide en 5 niveles de gestión: Directivo, Ejecutivo; Asesor, Apoyo y Operativo. Dentro del nivel directivo encontramos al Consejo Provincial el nivel ejecutivo lo conforma la Prefectura; el nivel asesor lo integran las Direcciones de Planificación , Relaciones externas, y el Departamento Jurídico; el nivel de Apoyo lo conforman las Direcciones Administrativa, Financiera, Secretaria General; dentro de los Niveles de Operativos encontramos a las Direcciones de Vías y Construcciones, Recursos Hídricos y gestión Ambienta, Producción, y Desarrollo Humano y Cultura.

Es importante señalar que la unidad de sistemas informáticos esta bajo la dependencia de la Dirección Administrativa, fungiendo las actividades de unidad técnica sobre la tecnología que abarca esta rama.

El H. Gobierno Provincial de Tungurahua está conformada por 3 dependencias físicas: El Edificio Principal ubicada en las calles Bolívar y Castillo, El edificio de Centro de Promociones y Servicios en las Calles Sucre y Castillo, La unidad de Talleres y Bodega del HGPT, ubicada en la Av. Gonzales Suarez y Av. América (Ingahurco) y en Catiglata Su estructura organizacional se divide en 5 niveles de gestión: Directivo, Ejecutivo; Asesor, Apoyo y Operativo. Dentro del nivel directivo encontramos al Consejo Provincial (Prefecto y Consejeros); el nivel ejecutivo lo conforma la Prefectura; el nivel asesor lo integran las Direcciones de Planificación , Relaciones externas, y el Departamento Jurídico; el nivel de Apoyo lo conforman las Direcciones Administrativa, Financiera, Secretaria General; dentro de los Niveles de Operativos

A continuación en el Grafico 6.10 se detalla el Estructura orgánica funcional del HGPT

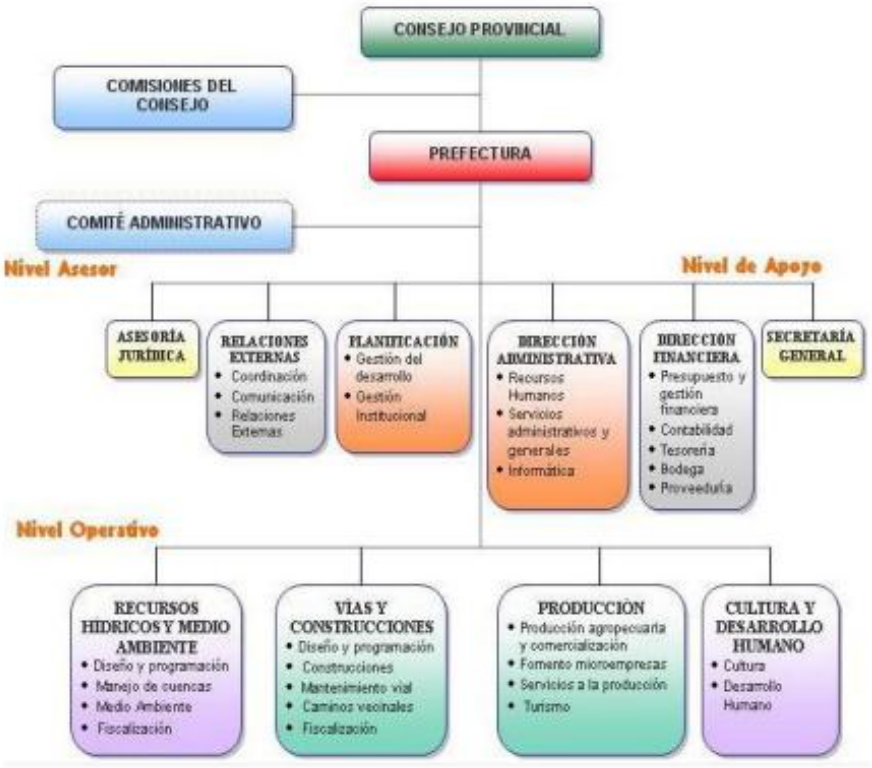


Gráfico Nº 6.10 Estructura Orgánica Funcional del HCPT

FUENTE: http://www.tungurahua.gob.ec/institucion/organigrama-estructural

A continuacion en los Graficos 6.11 y 6.12 se muestra la red del departamento de sistemas y del Centro de Promociones de la Provincia.

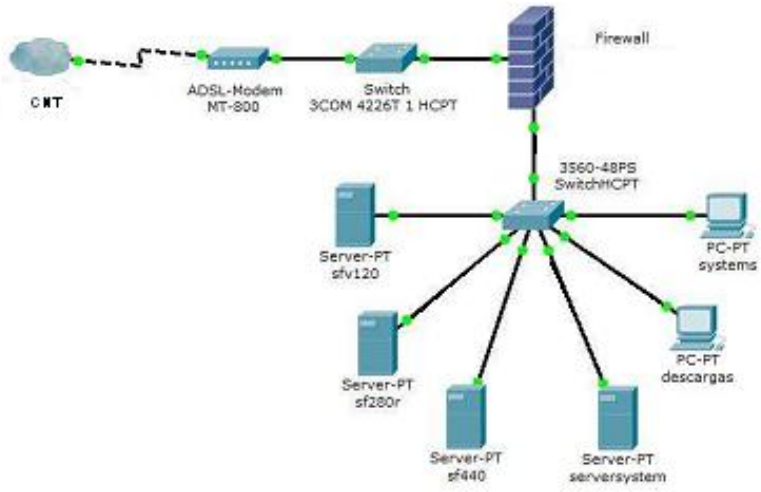


Gráfico Nº 6.11 Esquena departamento de Sistemas

FUENTE: Administrador del departamento de sistemas del HGPT

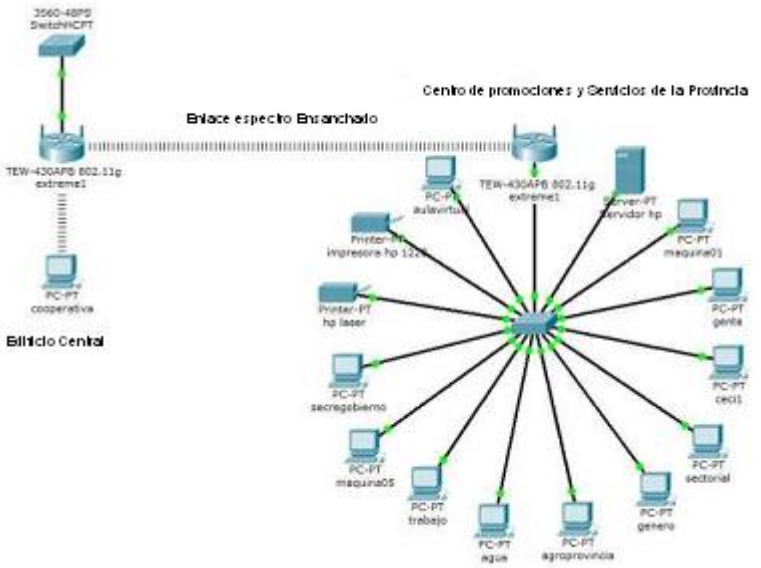


Gráfico Nº 6.12 Esquema de conexión Centro de Promociones y Servicios de la Provincia

FUENTE: Administrador del departamento de sistemas del HGPT

6.8.1 Diseño Físico de la conexión VPN entre el Departamento de Sistemas y las bodegas en Catiglata del HGPT

El servidor Openvpn fue colocado en las bodegas del HGPT, como se muestra en el Grafico 6.13, ya que asi se podrá tener acceso a toda la red de las bodegas, la IP externa del servidor con la cual sale a internet es la dirección publica 186.42.164.26, la IP interna del servidor es 172.16.0.65, la IP de túnel es 10.0.10.1 con máscara 255.255.255.0, y en el otro extremo en el departamento de sistemas la IP externa es 190.152.213.26, la IP interna es 172.16.1.146, la IP de túnel es 10.0.10.6 con máscara de 255.255.255.0

El servidor se conecta al Switch 3com 4226T, en el departamento de sistemas el cliente se conecta a Switch 3560 de 48 puertos.

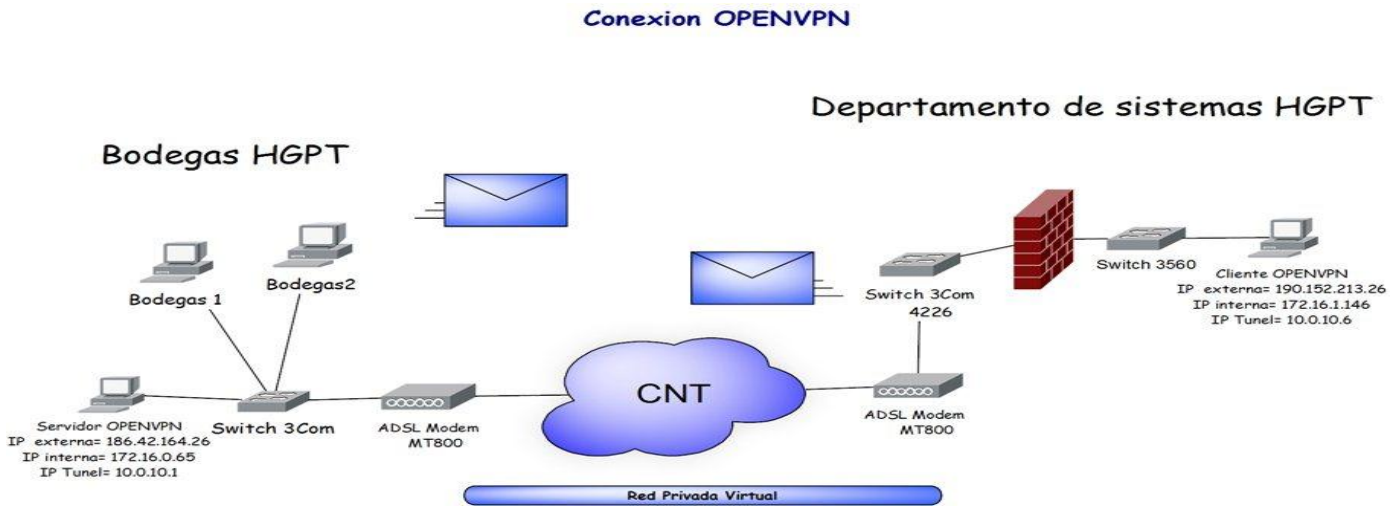


Gráfico Nº 6.13 Diseño de la Conexión VPN

Elaborado por: El investigador

6.8.2 Configuración de una VPN en Ubuntu 12.04 server y Windows 7

Aquí se explicara paso a paso la configuración de una conexión VPN que se la realizo con la ayuda de Openvpn, tanto en Ubuntu 12.04 como en Windows 7. Básicamente lo que se hizo fue una conexión a una red remota creando un túnel a través de internet, permitiendo la creación de una red privada dentro de una red pública.

6.8.2.1 Configuración VPN en Ubuntu 12.04

Antes de empezar la configuración hay que ver algunos comandos que van a servir en la consola de Ubuntu:

ls listar
rm borrar un archivo
cp copiar un archivo
pwd identificar el directorio en que se está
cd directorio cambia al directorio
cd .. Cambiar al directorio de nivel inferior
chown, chgrp, chmod, chattr, touch comandos para manejo de atributos de archivos
find, locate buscar archivos
grep buscar texto en archivos
Archivos comprimidos

tar -xvzf archivo Descomprime un archivo.tar.gz
tar -xvf archivo Descomprime un archivo.tar
gzip -d archivo Descomprime un archivo.gz
tar archivo archivo Empaqueta sin comprimir
gzip archivo Comprime archivos empaquetados
Manejo de archivos
ls -l Número de enlaces de un archivo

rm archivo Borrar enlaces, si no tiene enlaces, borra el archivo)

rm -r Borrar directorios

df Ver espacio libre en disco entero

find / -name mime.types Buscar un archivo

Sistema

/etc/init.d/boot Inicio del sistema

lsmod Ver módulos cargados en el kernel

Instalación

dpkg -i Instalar paquete

dpkg --info Información del paquete

dpkg -c Lista de archivos contenidos

dpkg --contents Lista todos los archivos contenidos con sus directorios

dpkg -f Informa versión del paquete

dpkg --unpack Desempaqueta

dpkg --purge Borra un paquete incluidos los archivos de configuración

dpkg -r Borra un paquete pero no borra los archivos de configuración

dpkg -L Lista el paquete si está instalado

dpkg -l Lista los paquetes instalados

La instalación de Ubuntu 12.04 server se la realizo en una computadora Core 2Quad con un procesador de 2.66Gz, ya que una vez concluidas las bodegas se adquirirá un servidor específicamente para esta función.

El proceso de instalación de Ubuntu 12.04 es algo muy sencillo es por eso que no se pondrá en este proyecto los pasos para la instalación.

Instalación y configuración del servidor mediante de Openvpn

Con la ayuda de Tunnelier, que es una herramienta que permite la conexión segura al servidor de las bodegas del HGPT mediante SSH, se ingresa a la consola del mismo para proceder con las respectivas configuraciones como se muestra en el Grafico 6.14:

La descarga e instalación se indicara en los anexos del proyecto

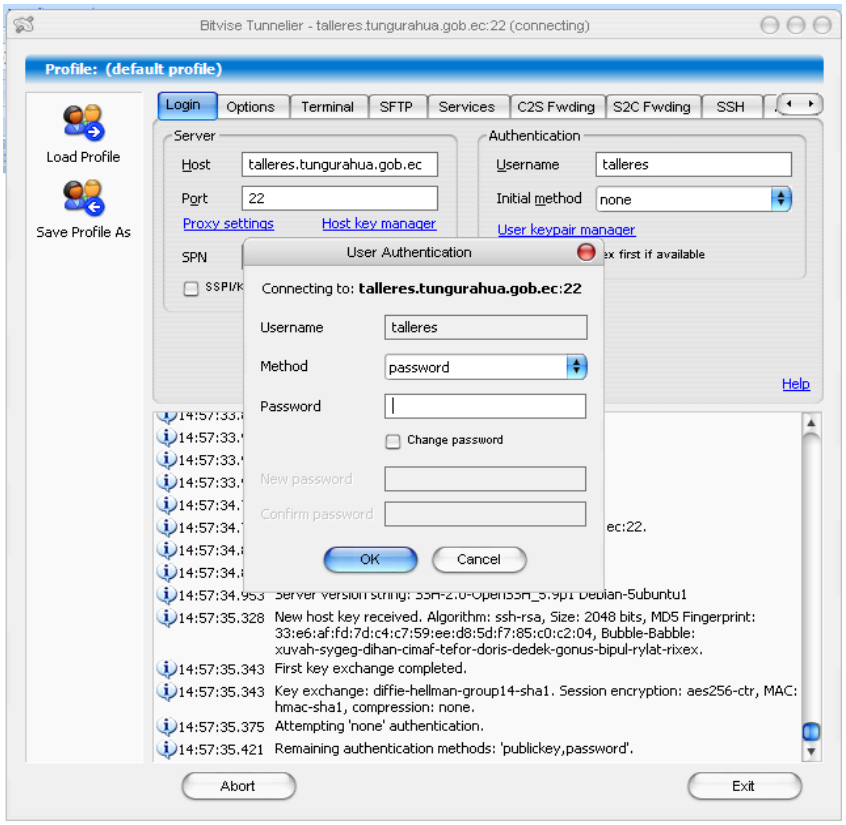


Gráfico Nº 6.14 Ingreso por SSH Mediante Tunnelier
Elaborado por: El investigador

Como Ubuntu esta basado en Debían La instalación de OpenVPN se la realiza mediante el comando “apt”. El sistema de gestión de paquetes APT simplifica la instalación y eliminación de programas en distribuciones tipo Debian. Para instalar OpenVPN mediante el comando “apt” se ha de introducir, simplemente, la siguiente línea de comando en un terminal de consola:

1.-Instalar OpenVPN y también OpenSSL, ya que la seguridad se basa en ssl.
Aplicar sudo para poder ingresar como usuarios root
sudo apt-get -y install openvpn
sudo apt-get -y install openssl
Como se muestral en el Grafico 6.15

Gráfico Nº 6.15 Instalación paquetes Openvpn

Elaborado por: El investigador

2.-Ingresar al directorio /usr/share/doc/openvpn/examples, y copiar las carpeta easy-rsa donde se encuentran los archivos de configuracion de openvpn con el comando **cp –R easy-rsa** , hacia el directorio /etc/openvpn,

Lo que hace el comando **cp –R** es copiar todo lo que se encuentre en el directorio que se indique hacia otro directorio o carpeta

3.-En el directorio usr/share/doc/openvpn/examples, ingresar a la carpeta simple-config-files, como se muestra en el Grafico 6.16

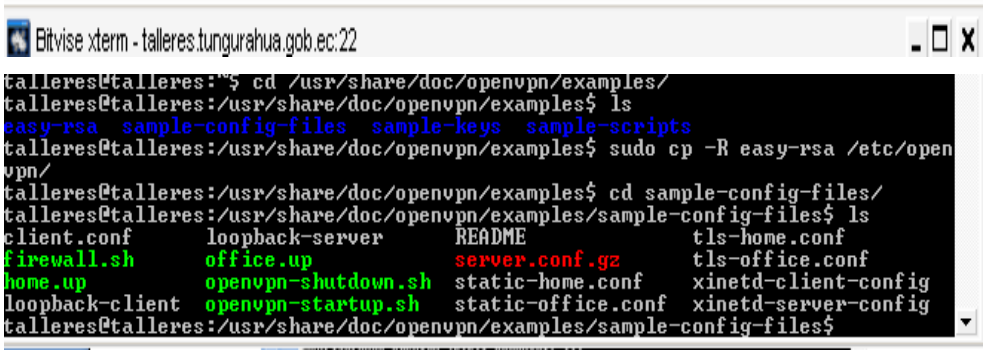


Gráfico Nº 6.16 Configuración openvpn1

Elaborado por: El investigador

4.-De igual manera copiar los archivos server.conf.gz y client.conf al directorio /etc/openvpn. Como se muestra en el Grafico 6.17

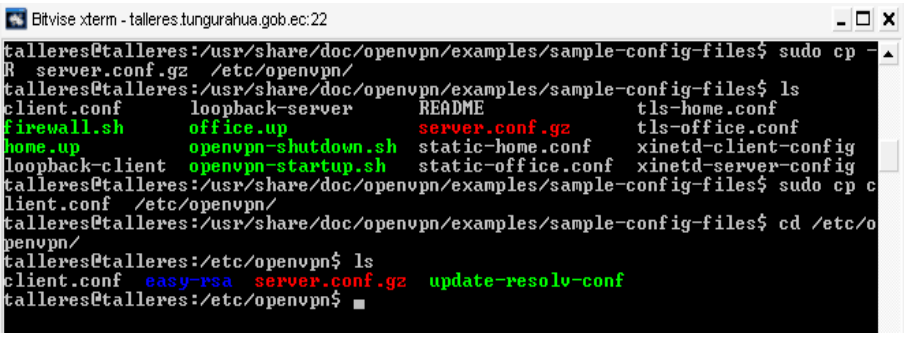


Gráfico Nº 6.17 Configuración openvpn2

Elaborado por: El investigador

4.-En el directorio /etc/openvpn ingresar a la carpeta easy-rsa en la cual van a encontrar dos carpetas 1.0 y 2.0, vamos a ingresar en la carpeta 2.0, como se muestra en el Grafico 6.18

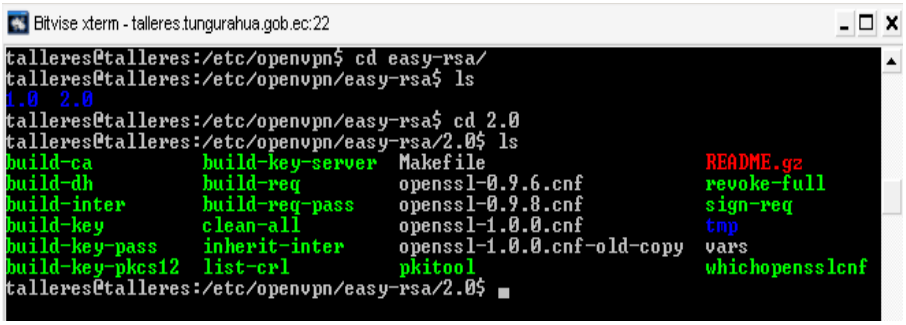


Gráfico Nº 6.18 Configuración openvpn3

Elaborado por: El investigador

5.-Editar el archivo vars con el comando **sudo nano vars** y cambiar la línea que dice:

export KEY_CONFIG="$EASY_RSA/wichopensslcnf $EASY_RSA" y la cambiamos por:

export KEY_CONFIG=/etc/openvpn/easy-rsa/2.0/openssl-1.0.0.conf

Una vez hecho esos cambios presionar ctr+o para guardar y luego ctr+x para salir. Como se muestra en el Grafico 6.19

Gráfico Nº 6.19 Configuración openvpn4

Elaborado por: El investigador

6.-Regresar al directorio /etc/openvpn/easy-rsa y con el comando **sudo chmod 777 2.0.** dan los permisos de lectura, escritura y ejecución a la carpeta 2.0, que se encuentra en easy-rsa.

Regresar al directorio /easy-rsa/2.0 y ejecutar el siguiente comando: **. ./vars** (el comando es un punto, espacio y otro punto, seguido de /vars) . Y aparecerá la siguiente nota:

NOTE: If you run ./clean-all, i will de doing a rm –rf on /etc/openvpn/easy-rsa-V2.0/keys

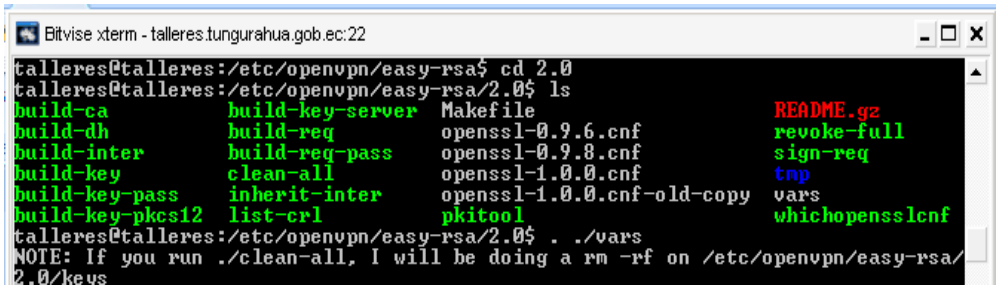


Gráfico Nº 6.20 Configuración openvpn5

Elaborado por: El investigador

7.-Ahora hay que configurar un entorno nuevo borrando potenciales archivos viejos ejecutando , **. /clean-all** (hay que recordar que esta configuración se la realiza únicamente dentro de easy-rsa/2.0). Después poner el comando **./buid-ca** con esto se crea la unidad certificadora.

En este punto lo que se va hacer es colocar los datos que se acoplen mejor a la seguridad de la empresa: como por ejemplo

Country Name: EC

State or Province: TU

Locality Name: Ambato

Organization name: Hgpt

Organization Unit name: tungurahua.gob.ec

Common Name: talleres.tungurahua.gob.ec

Name: Administrador

Tal como se muestra en el Grafico 6.21

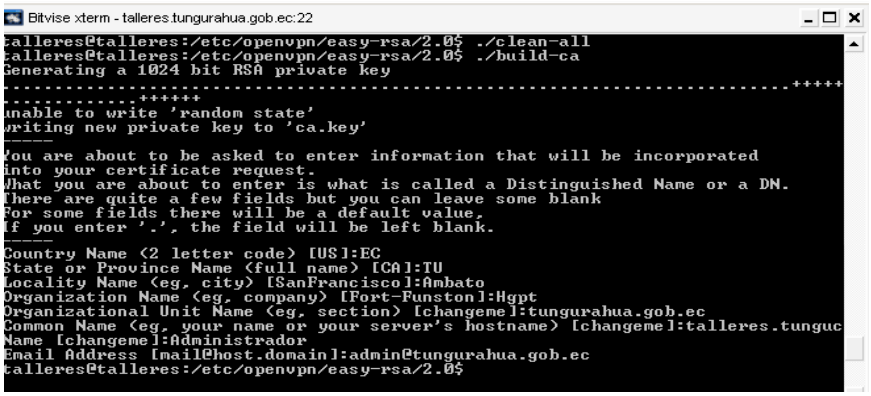
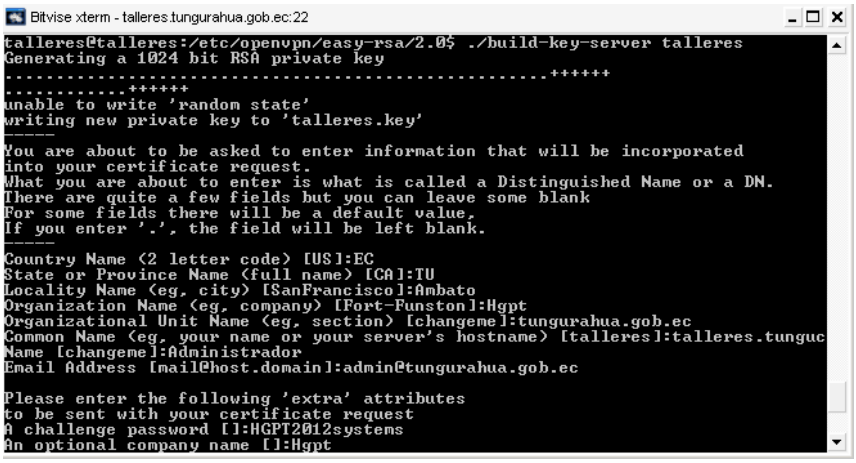


Gráfico Nº 6.21 Configuración openvpn6

Elaborado por: El investigador

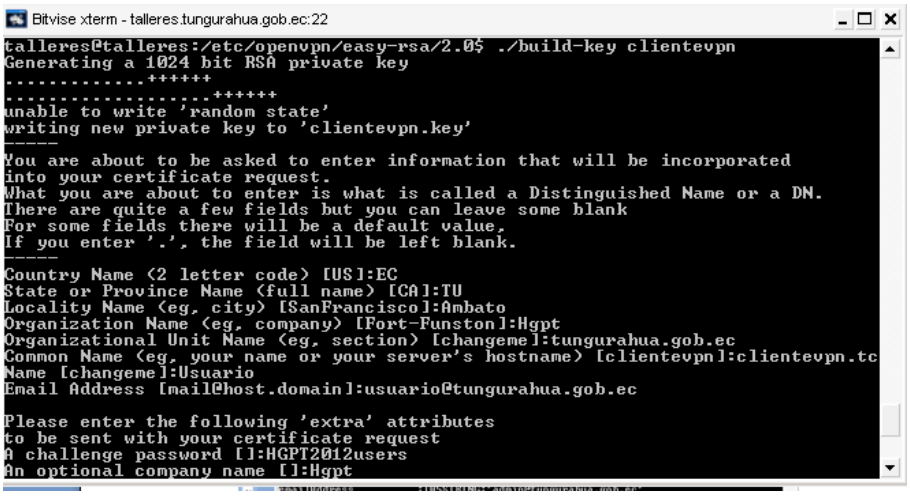
8.-Una vez creado el Certificate Authority (CA) crear la llave del servidor con el comando **./build-key-server nombre del servidor** en el cual hay que llenar los mismos parámetros que en la CA con la diferencia que en Common Name poner el nombre del servidor en nuestro caso es talleres, como se muestra en el Grafico 6.22



Con este paso se crearon los archivos (talleres.crt, talleres.key, talleres.csr)

Gráfico Nº 6.22 Configuración openvpn7 **Elaborado por:** El investigador

9.-Ahora hay que generar las claves de los clientes con el comando **./build-key nombre del cliente**, hay que ejecutar lo mismo para cada uno de los clientes, de igual los parámetros que van a cambiar es Common Name y Name, en nuestro caso es clientevpn y Usuario respectivamente, como se muestra en el Grafico 6.23

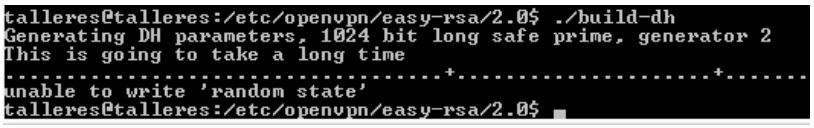


Esto va a generar que se cree (clientevpn.crty, clientevpn.key, clientevpn.csr)

Gráfico Nº 6.23 Configuración openvpn8

Elaborado por: El investigador

10.-Crear los parámetros Diffie-Hellman, con esto se termina de implementar la seguridad de este escenario, lo que hace es cifrar matemáticamente todo el proceso



Con esto en el directorio /etc/openvpn/easy-rsa/2.0 se crea una carpeta con los datos del servidor y de los clientes cliente con el nombre de Keys

Gráfico Nº 6.24 Configuración openvpn9
Elaborado por: El investigador

11.-Ahota hay que dar permiso de lectura, escritura y ejecución a la carpeta Keys (hay que recordar que estan en este directorio /etc/openvpn/easy-rsa/2.0) ya que se necesita copiar los archivos: en nuestro caso talleres.crt (certificado del servidor), talleres.key (clave privada del servidor), dh1024.pem al directorio /etc/openvpn, como se muestra en el Grafico 6.25

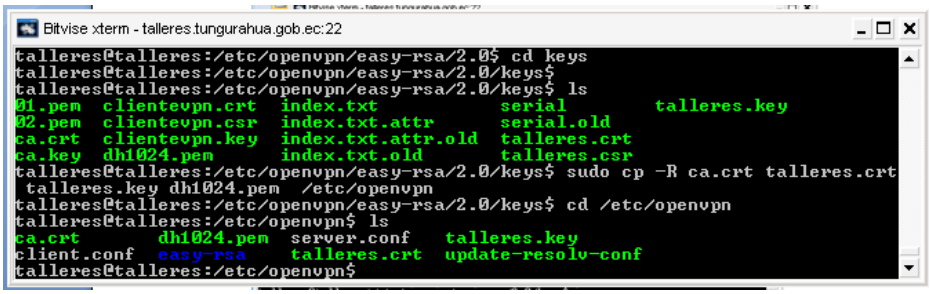


Gráfico Nº 6.25 Configuración openvpn10
Elaborado por: El investigador

12.-Una vez copiados los archivos ingresar al directorio /etc/openvpn y editar el archivo server.conf con el comando sudo **nano server.conf** y lo que tiene que quedar es lo siguiente:

dev tun

proto udp

port 1194

ca ca.crt

cert talleres.crt

key talleres.key

dh dh1024.pem

user nobody

group nogroup

server 10.0.10.0 255.255.255.0

ifconfig-pool-persist /etc/openvpn/clients.txt

persist-key

persist-tun

push "route 172.16.0.64 255.255.255.224"

keepalive 10 120

verb 3

comp-lzo

max-clients 3

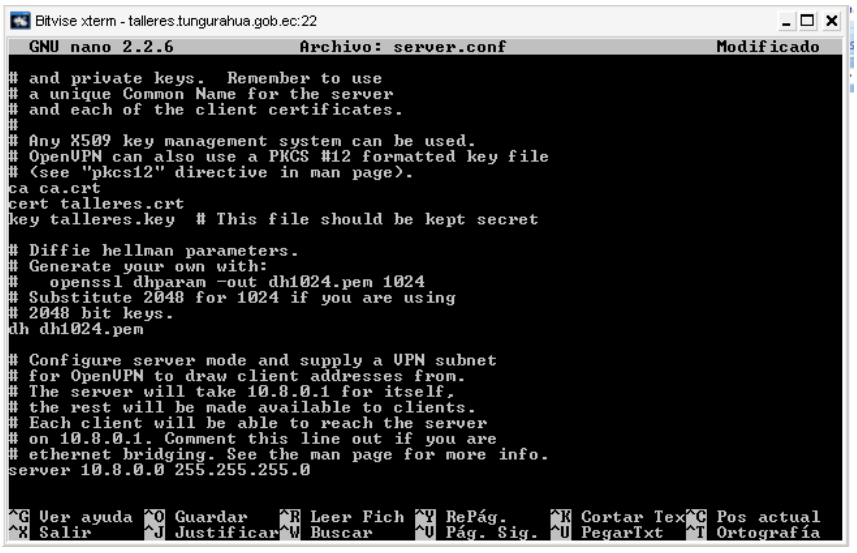


Gráfico Nº 6.26 Configuración openvpn11

Elaborado por: El investigador

13.-Ahora hay que instalar la herramienta Samba la cual ayudara para compartir archivos con la red, la instalación se lo realiza con el comando **sudo apt-get –y install samba samba-client smbfs smdclient** como se muestra en el Grafico 6.27

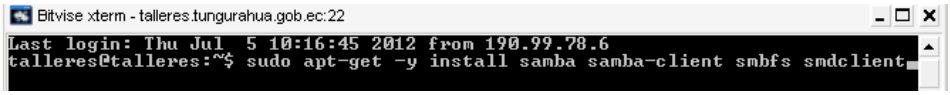


Gráfico Nº 6.27 Instalación de Samba

Elaborado por: El investigador

14.-Crear la carpeta que se va a compartir en la red, en la cual se encuentran los archivos de configuración de cliente, y se lo hace con el siguiente código **sudo nano /etc/samba smb.conf.**

A continuación colocar lo siguiente como se nuestra en el Grafico 6.27

[Compartir]

path = /usr/compartir

public = yes

writable = no

Lo guardamos y salimos.

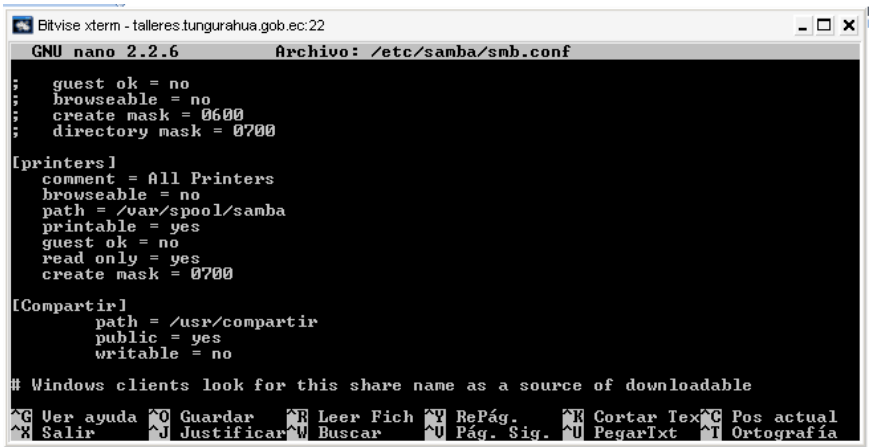


Gráfico Nº 6.27 Instalación de Samba

Elaborado por: El investigador

15.-Crear una carpeta con el nombre de compartir en la carpeta usr con el comando **sudo mkdir /usr/compartir,** luego ir al directorio /etc/openvpn/easy-rsa/ y copiar los archivos ca.crt ca.key talleres.ctr talleres.key clientevpn.crt clientevpn.key al directorio /usr/compartir, como se muestra en el Grafico 6.28.

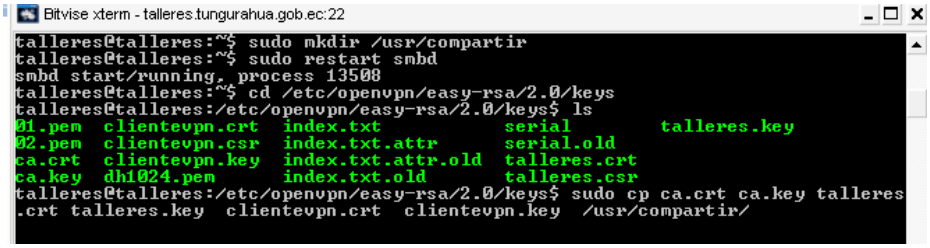
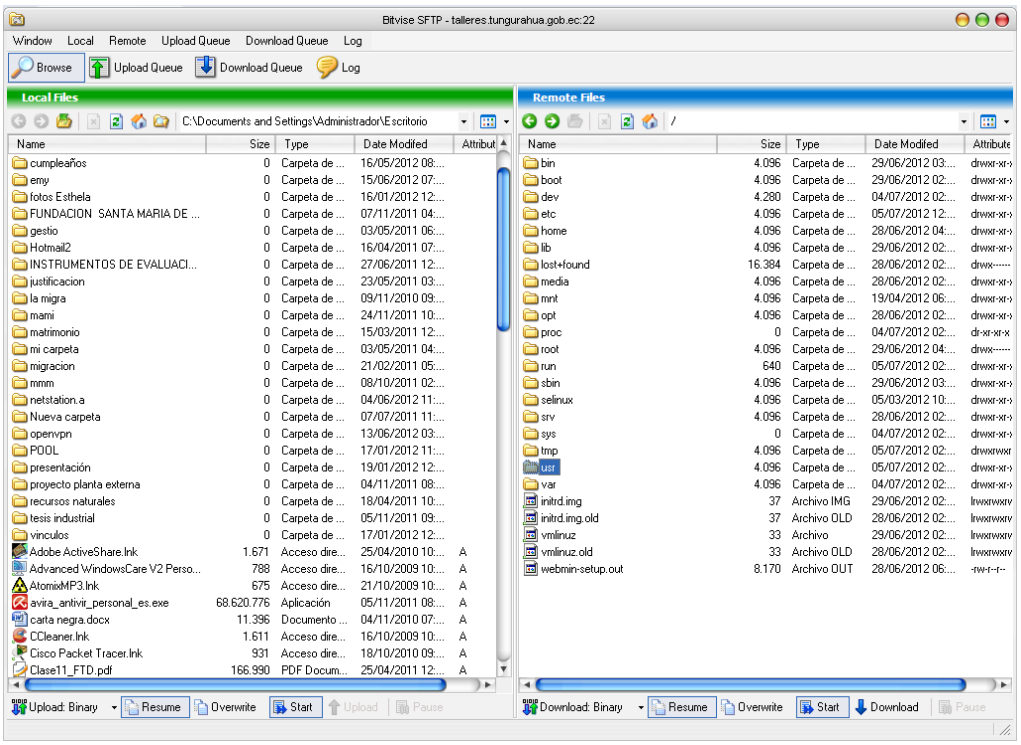


Gráfico Nº 6.28 Compartición de archivos
Elaborado por: El investigador

16.-Otra manera de compartir los archivos para los clientes es mediante Tunnelier ya que permite interactuar de manera grafica con los archivos y carpetas del servidor VPN, como se muestra en el Grafico 6.29



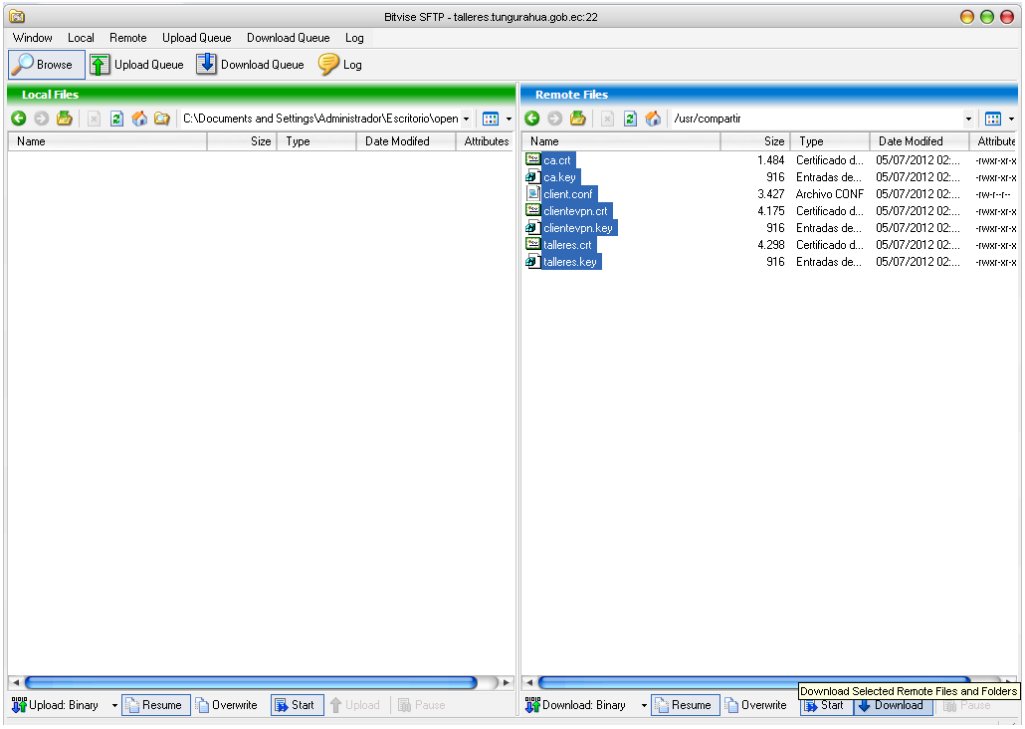


Gráfico Nº 6.29 Compartición de archivos con Tunnelier

Elaborado por: El investigador

6.8.2.2 Configuración VPN en Windows 7

Para la configuración en Windows se necesita de Openvpn (aplicación para windows 7) la cual indicara en los anexos su página de descarga e instalación.

17.-Una vez descargado Openvpn y los archivos de configuración del cliente VPN Hay que ingresar en la maquina del cliente en Inicio/Equipo/Disco local C:/Archivos de programa/Openvpn/config, y pegar ahí los archivos que se descargue del servidor VPN, como se muestra en el Grafico 6.30

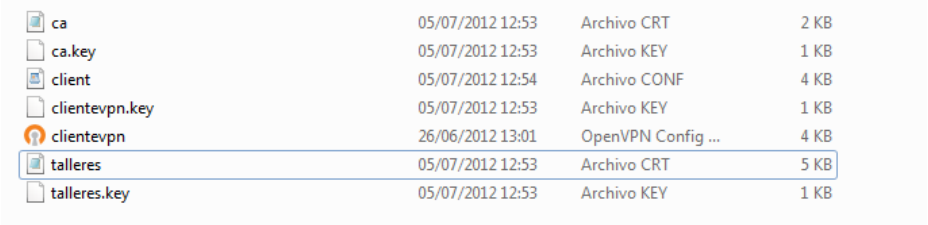


Gráfico Nº 6.30 Archivos de configuración clientevpn

Elaborado por: El investigador

18.-El archivo client editarlo y renombrarlo como clientevpn.ovpn (.ovpn extencion de openvpn en windows) el mismo que tiene la siguiente configuración

client

dev tun

proto udp

remote talleres.tungurahua.gob.ec 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert clientevpn.crt

key clientevpn.key

ns-cert-type server

comp-lzo

verb 3

19.-Ejecutar Openvpn como administrador , como se muestra en el Grafico 6.31 ya que no tendría los privilegios para enviar y recibir la información que llega a través del túnel, una vez ejecutado en la parte inferior derecha en la barra de herramientas del escritorio aparecerá una imagen de una computadora de color roja 

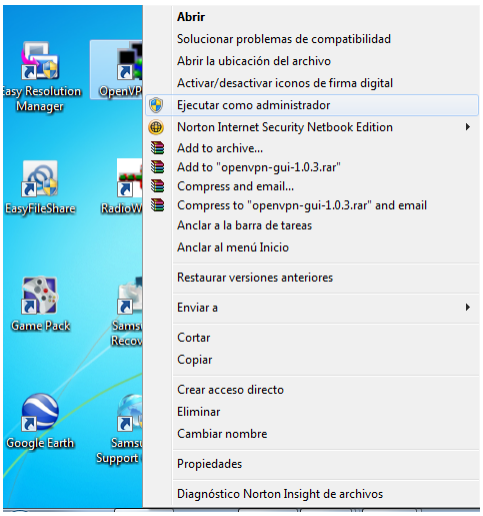


Gráfico Nº 6.31 Openvpn como administrador

Elaborado por: El investigador

20.-Hay que darle click derecho a la imagen  y aparecera un menu, en el cual hay que darle click en Conect para que asi establezca la conexión con el servidor y asi le asigne una direccion valida , como se muestra en el Grafico 6.32.

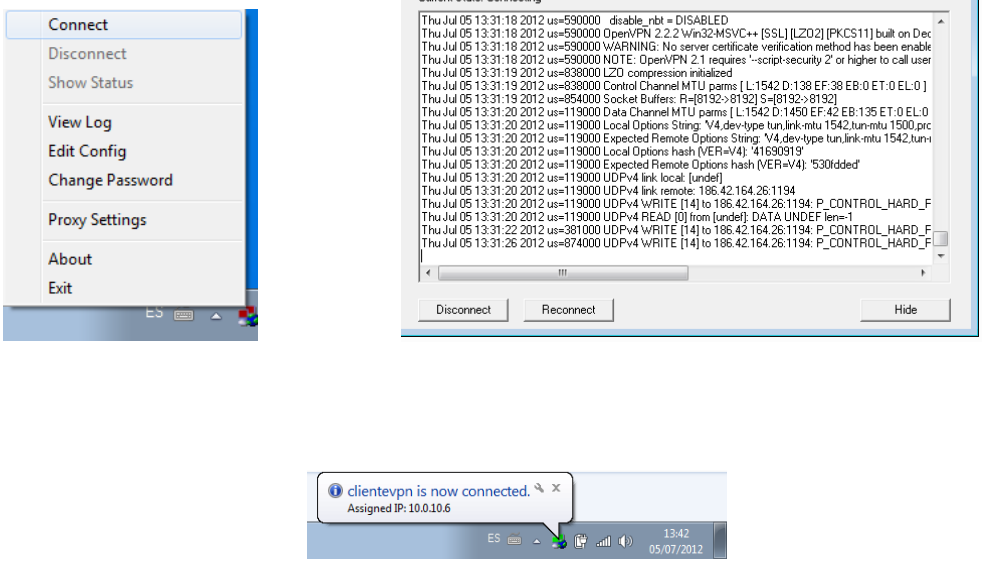


Gráfico Nº 6.32 Conexión clientevpn

Elaborado por: El investigador

6.8.2.3 Pruebas de conexión

Las pruebas de conexión se las realizaron haciendo un ping desde el clientevpn hacia el servidor VPN y hacia la red LAN del servidor VPN, también se puede comprobar la conexión dando Inicio/Ejecutar: y colocando la dirección del servidor VPN, ahí se aparecerá una carpeta con los archivos compartidos por el servidor.

a) Haciendo ping a la ip 10.0.10.1, como se muestra en el Grafico 6.33

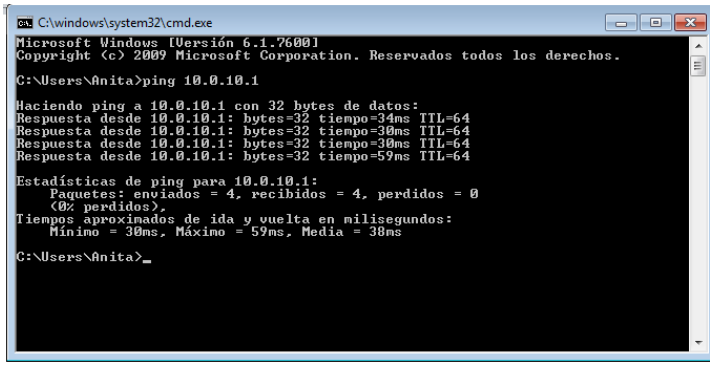


Gráfico Nº 6.33 Prueba de conexión mediante Ping al servidor

Elaborado por: El investigador

b) Haciendo ping a la red LAN del servidor, como se muestra en el Grafico 6.34

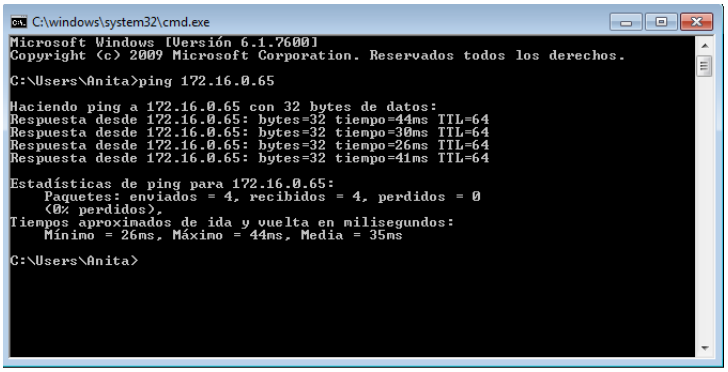
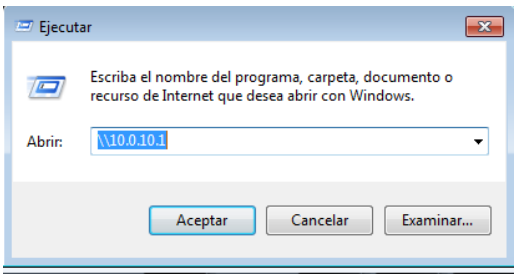
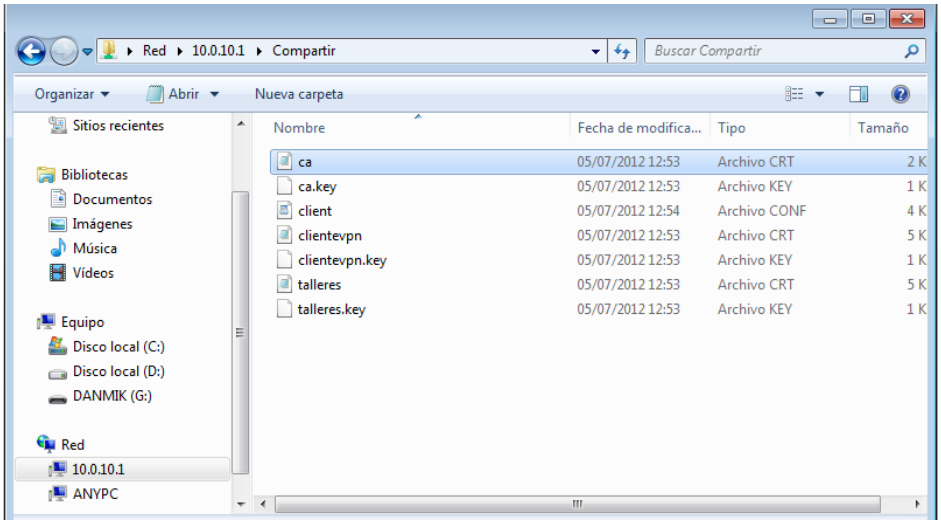


Gráfico Nº 6.34 Prueba de conexión mediante Ping a la red LAN

Elaborado por: El investigador

a) Inicio/Ejecutar, como se muestra en el Grafico 6.35





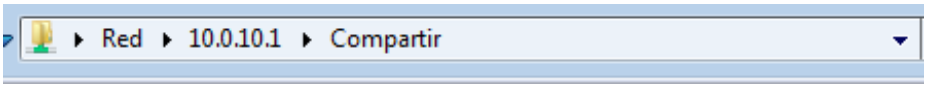


Gráfico Nº 6.35 Prueba de conexión mediante Ejecutar
Elaborado por: El investigador

6.8.3 Configuración de Asterisk en Ubuntu 12.04

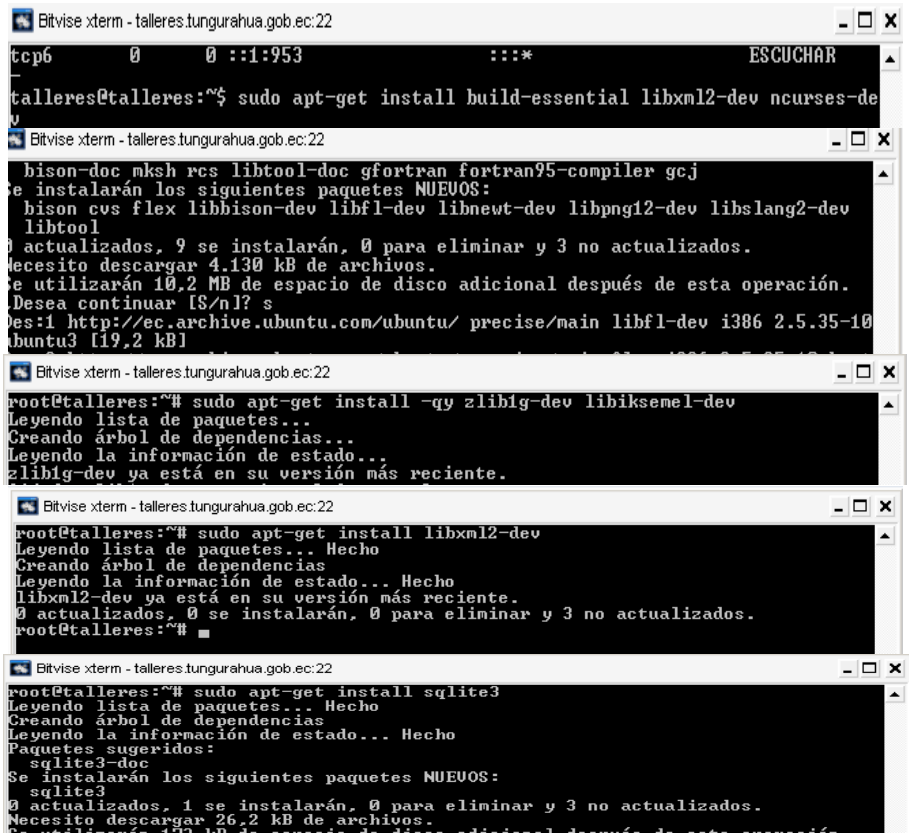
Primeramente para poder configurar Asterisk en Ubunto hay que obtener una versión de Asterisk que permita ser actualizada y sea compatible en un futuro con otras versiones.

Para la configuración de Asterisk también se hace uso de Tunnelier.

1.-Antes de instalar Asterisk en Ubuntu se debe instalar unas dependencias que son necesarias para su correcto funcionamiento, y lo hacemos de la siguiente manera:

- sudo apt-get install build-essential libxml2-dev ncurses-dev
- sudo apt-get install bison ncurses-dev libssl-dev libnewt-dev cvs procps debhelper dpkg-dev gettext html2text po-debconf build-essential automake flex libtool libncurses5-dev libssl-dev
- sudo apt-get install -qy zlib1g-dev libiksemel-dev
- sudo apt-get install libxml2-dev
- sudo apt-get install sqlite3
- sudo apt-get install sqlite3 libsqlite3-dev
- sudo apt-get install rubygems1.9.1
- sudo apt-get install ruby-full build-essential
- sudo aptitude install ruby build-essential libopenssl-ruby ruby 1.8-dev
- sudo gem install sqlite3-ruby

Una vez instaladas las dependencias poner el comando sudo **apt-get update** para que se actualice los repositorios de Ubuntu y sudo **apt-get upgrade** si es que hay nuevos los instala, como se muestra en el Grafico 6.36



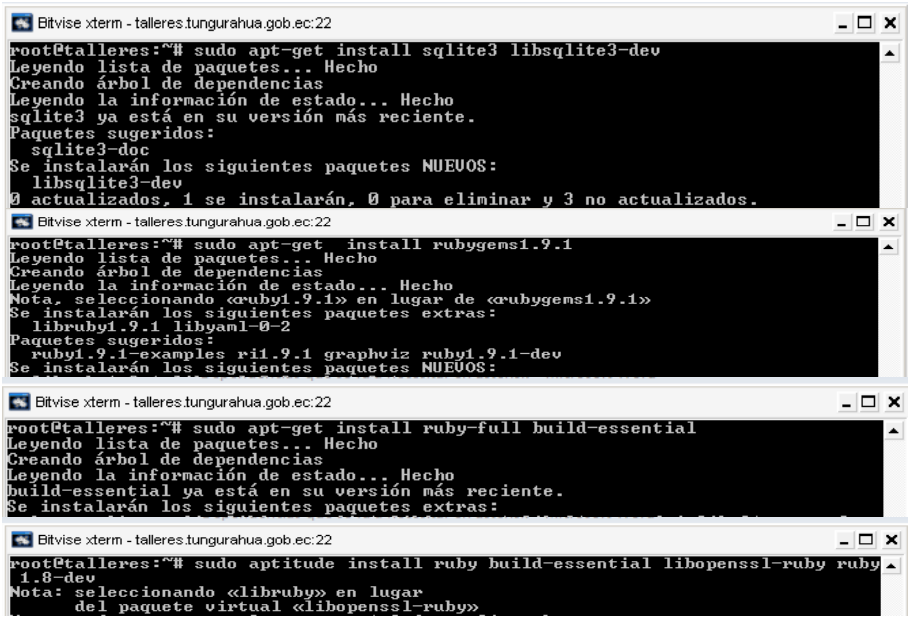


Gráfico Nº 6.36 Dependencias de Asterisk
Elaborado por: El investigador

2.-Para continuar con la configuración convertirse en usuario root con el comando **sudo su**. Para la decodificación de archivos Mp3 se lo encuentra en el directorio /usr/src y se procede a descargar el complemento con el siguiente comando **wget http://cdnetworks-us-2.dl.sourceforge.net/project/npg123/mpg123/1.13.4/mpg123-123-1.13.4.tar.bz2,** como se muestra en el Grafico 6.37

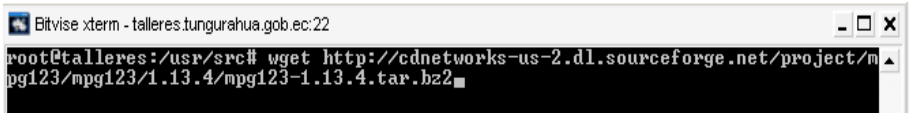


Gráfico Nº 6.37 Descarga decodificador de archivos Mp3
Elaborado por: El investigador

3.- En el directorio /usr/src proceder a descargar Asterisk, y se lo hace de la misma manera que en el punto 2: wget http://downloads.asterisk.org/pub/telephony/certified-asterisk/releases/certified-asterisk-1.8.11-cert2.tar.gz, como se muestra en el Grafico 6.38

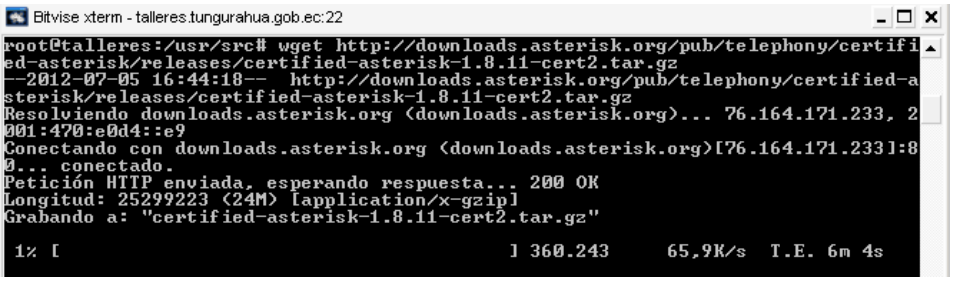


Gráfico Nº 6.38 Descarga Asterisk

Elaborado por: El investigador

4.-Una vez descargado Asterisk y mpg123, archivos que se encuentran en directorio /usr/src en formato tar.gz y tar.bz2 respectivamente, procedemos a descomprimirlos y lo realizamos con los comandos

tar - xvzf certified-asterisk-1.8.11-cert2.tar.gz.tar y

tar –xjvf mpg123-1.13.4.tar.bz2

Como se muestra en el Grafico 6.39

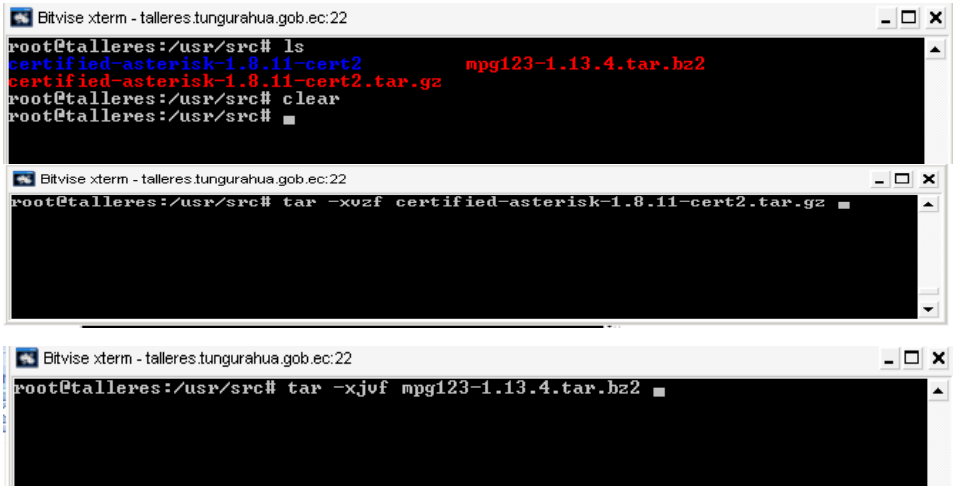


Gráfico Nº 6.39 Descomprimir archivos *gz.tar* y *gz.bz2*

Elaborado por: El investigador

5.-Ingresar al directorio /usr/src/mpg123-1.13.4 y configurar mpg123 con el siguiente comando **./configure** luego el comando **make** y por último el comando **make install.**

6.-Ingresando en el directorio **/usr/src/certified-asterisk-1.0.11-cert2** se procede a configurar y a instalar Asterisk de igual manera con el comando **./configure** con este comando se validarán las librerías y dependencias de nuestro servidor para que Asterisk pueda ser compilado, como se muestra en el Grafico 6.40

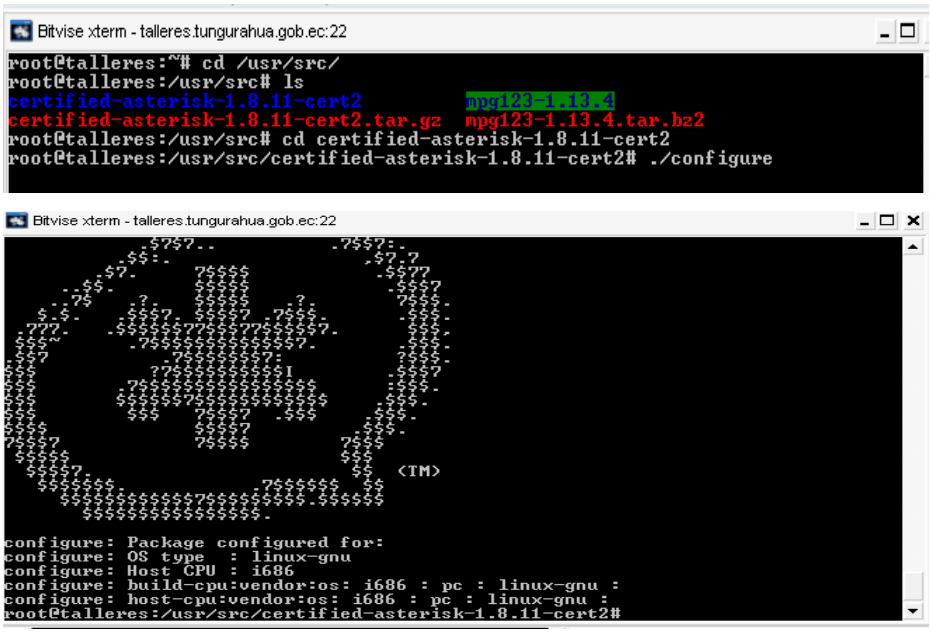


Gráfico Nº 6.40 ./configure

Elaborado por: El investigador

7.-Ejecutando make menuselect se abrirá una ventana como esta Grafico 6.41:

Gráfico Nº 6.41 Módulos de Asterisk

Elaborado por: El investigador

8.-Aquí se selecciona los módulos a cargar en Asterisk, por ahora únicamente ir a Core Sound Packages y Extra Sound Packages, allí habilitar la opción **CORE-SOUNDS-ES-GSM y EXTRA-SOUNDS-EN-GSM** respectivamente (para seleccionar se utiliza la barra espaciadora). Una vez terminado guardar y salir, como se muestra en el Grafico 6.42

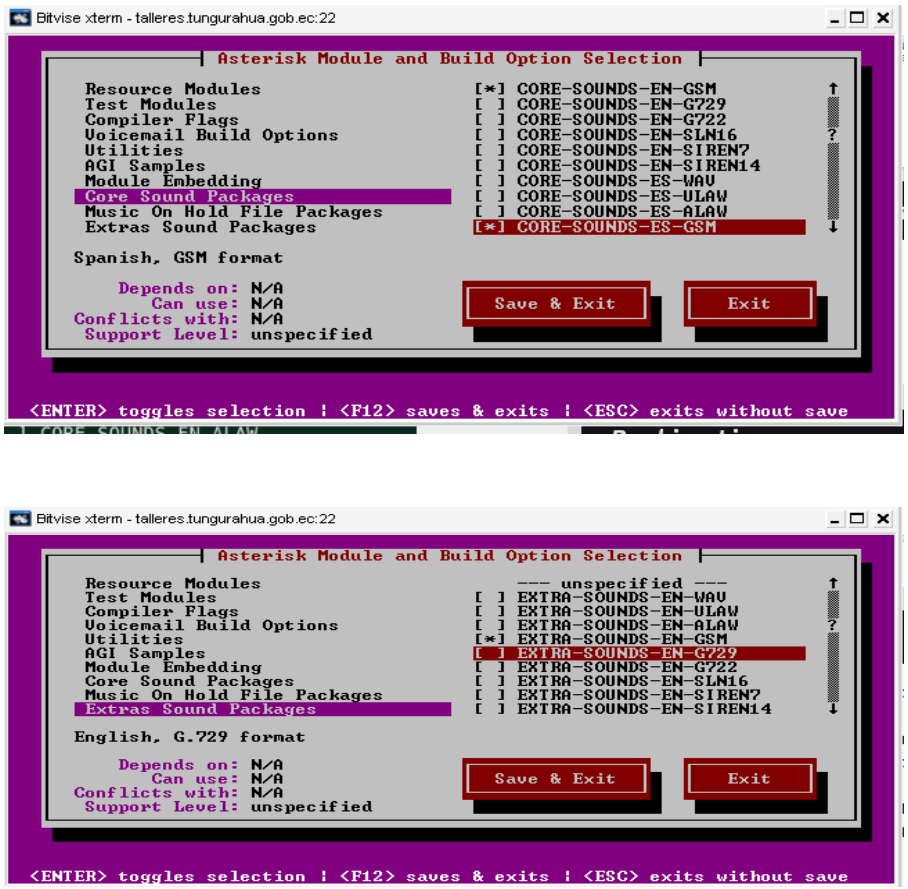


Gráfico Nº 6.42 Modulos de Asterisk 1

Elaborado por: El investigador

9.-Para soporte de MP3 hay que instalar subversión con el comando **apt-get install subversión,** luego ingresar al directorio /usr/src/certified- asterisk-1.0.11-cert2 y ejecutar el comando **contrib/scripts/get_mp3_source.sh,** como se muestra en el Grafico 6.43.

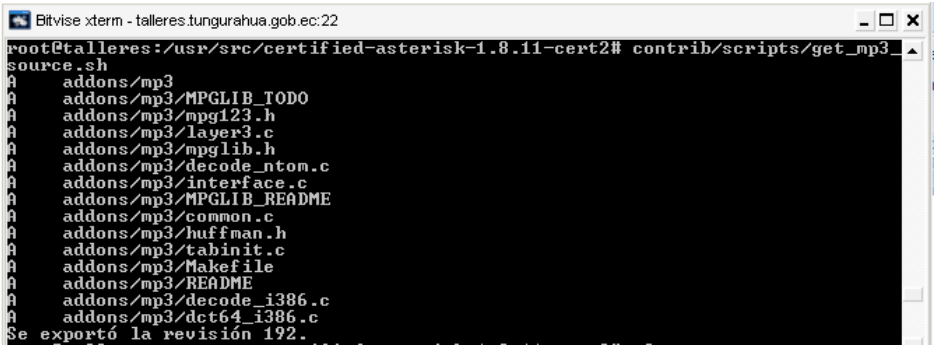


Gráfico Nº 6.43 Instalación Soporte MP3

Elaborado por: El investigador

10.-Ejecutar los siguientes comandos para compilar asterisk

- Compilamos con **make**
- Instalamos programas y módulos con **make install**
- Instalamos los archivos de ejemplo de asterisk con **make samples**
- Instalamos los scripts para que asterisk inicie con nuestro servidor tras los reinicios con **make config**
- Instalamos logrotate para la rotación de los logs **make install-logrotate**

11.-Se inicia el servicio de Asterisk con el comando **/etc/init.d/asterisk start,** como se muestra en el Grafico 6.44

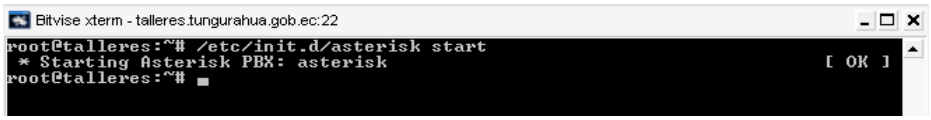


Gráfico Nº 6.44 Inicio servicio Asterisk

Elaborado por: El investigador

12.-Ingresar al directorio /etc/asterisk y Modificar el archivo de configuración sip.conf por sip.conf.ori, esto se lo hace para no perder el archivo original de configuración, luego se crea un nuevo archivo de configuración con el nombre de sip.conf, esto se lo hace para poder entender de una mejor manera los parámetros

de sip.conf, y se lo realiza con el comando **mv sip.conf sip.conf.ori (cambiar de nombre) y nano sip.conf(crear un nuevo sip.conf)** como se muestra en el Grafico 6.45

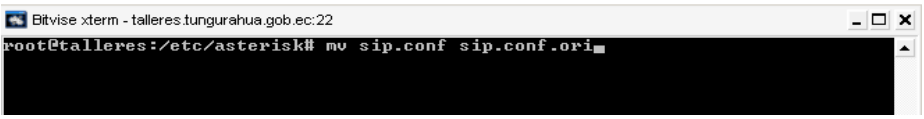


Gráfico Nº 6.45 Renombrando al archivo sip
Elaborado por: El investigador

13.-En el archivo sip.conf poner la siguiente configuración, como se muestra en el Grafico 6.46

sip.conf
[general]
context=default
allowguest=no
srvlookup=yes
udpbindaddr=0.0.0.0
transport=udp

[telefono1]
type=friend
secret=c0ntras3!
host=dynamic
insecure=port,invite
context=users

[telefono2]
type=friend
secret=h0tf1x3d2012
host=dynamic

insecure=port,invite

context=users

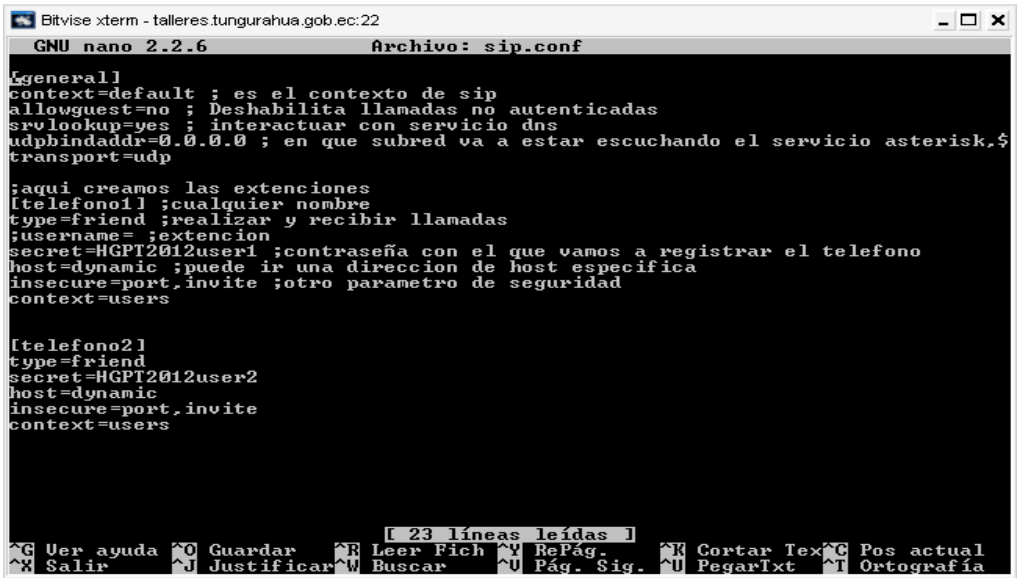


Gráfico Nº 6.46 Sip.conf

Elaborado por: El investigador

14.-En la misma extensión /etc/asterisk al igual que la configuración anterior cambiar el nombre al archivo **extensions.conf** por **extensions.conf.ori.** Ahora se crea otro archivo con el comando nano **extensions.conf**. Como se muestra en el Grafico 6.47

[general]

static=yes

writeprotect=no

autofallthrough=yes

clearglobalvars=no

priortityjumping=no

[globals]

;Los contextos comienzan acá

[users]

exten => 2001,1,Dial(SIP/telefono1,20)

exten => 2002,1,Dial(SIP/telefono2,20)

exten => 9998,n,Goto(menu1,s,1)

Este es el código para el menú:

[menu1]

exten => s,1,Answer()

exten => s,n,Wait(1)

exten => s,n,Background(press-1)

exten => s,n,Background(or)

exten => s,n,Background(press-2)

exten => s,n,WaitExten(3)

exten => 1,1,Playback(you-entered)

exten => 1,n,Playback(digits/1)

exten => 1,n,Goto(s,1)

exten => 2,1,Playback(you-entered)

exten => 2,n,Playback(digits/2)

exten => 2,n,Goto(s,1)

exten => h,1,NoOP(hey, han colgado la llamada!!!)

exten => h,n,Hangup()

exten => t,1,Playback(too-low)

exten => t,n,Goto(s,1)

exten => i,1,Playback(pbx-invalid)

exten => i,n,Hangup()

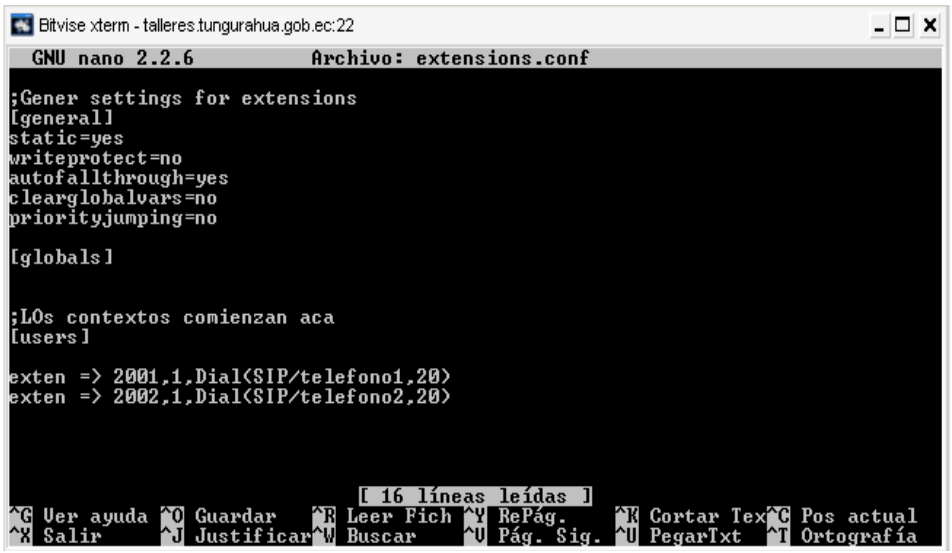


Gráfico Nº 6.47 Extensions.conf

Elaborado por: El investigador

En el archivo de configuración extensions.conf se configura el plan de marcado y el comportamiento de todas las conexiones a través del IP PBX: este controla, como se gestionan y encaminan las llamadas entrantes y salientes del sistema Asterisk

15.-Una vez configurado los archivos sip.conf y extentensions.conf hay que ingresar a la CLI de Asterisk que se encuentra en /etc/asterisk/ y se colaca el comando **asterisk –rvvv.**
En la Cli dar el comando **sip reload** para recargar la configuración de Sip y **dialplan reload** para cargar la configuración de dialplan

6.8.4 Configuración del Sofphone en Windows 7

El sofphone es la aplicación o archivo que se utiliza para poder hacer las llamadas desde la Pc. Este Softphone se llama X-LITE, es el más avanzado sistema de comunicación por ip y voip. Su modelo especial es fácil de manejar y configurar.

1.-Ya instalado X-lite hay que configurar la cuenta del cliente. Se selecciona Sofphone en el menú principal, ubicado en la parte superior del programa, donde aparecerá la opción Account Settings, como se muestra en el Grafico 6.48

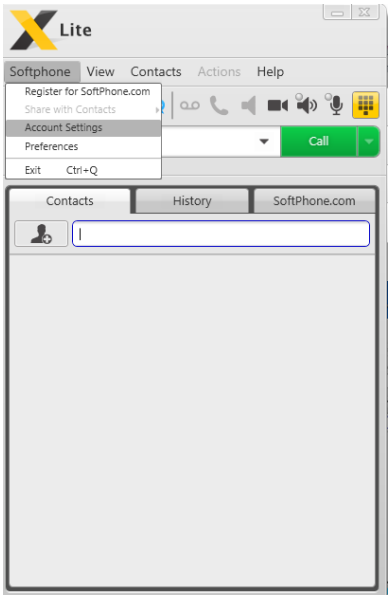


Gráfico Nº 6.48 X-Lite Account Settings **Elaborado por:** El investigador

2.-Posteriormente aparecerá una ventana denominada SIP Account en la pestaña cuenta, se configura la información proporcionada por el servidor Asterisk la cual es la siguiente:

- **Account name**: Es el nombre del usuario la cuenta.
- **User ID**: Es el nombre que le asignamos en Sip.conf
- **Domain**: Es el dominio o Servidor proxy para conectarse a la red de la empresa que provee la Telefonía IP
- **Password**: Es la contraseña que si le asigno al teléfono en sip.conf
- **Display name**: Es la información que aparecerá en la pantalla del Softphone XLite.
- **Authorization name:** Es el nombre que le asignamos en Sip.conf [26]

Adicionalmente debe estar marcado el checkbox: Register with domain and receive calls, de misma forma el botón Domain. Como se muestra en el Grafico 6.49

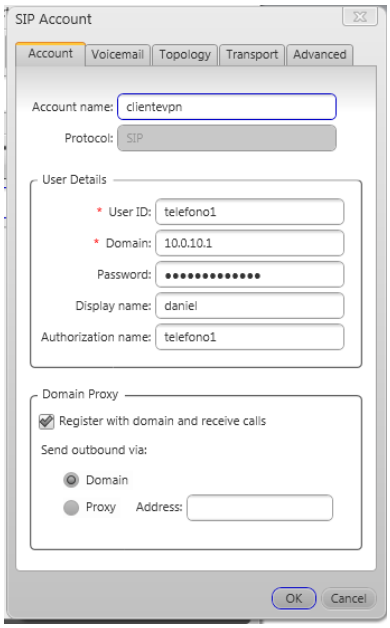


Gráfico Nº 6.49 X-Lite Account

Elaborado por: El investigador

[26] http://repositorio.espe.edu.ec/bitstream/21000/4845/1/T-ESPE-032947.pdf

3.-A continuación el Softphone X-Lite tratará de registrarse (login) con el servidor de Asterisk. Se puede observar que esto sucede en pocos segundos y si el registro tiene éxito, se observará la siguiente pantalla.

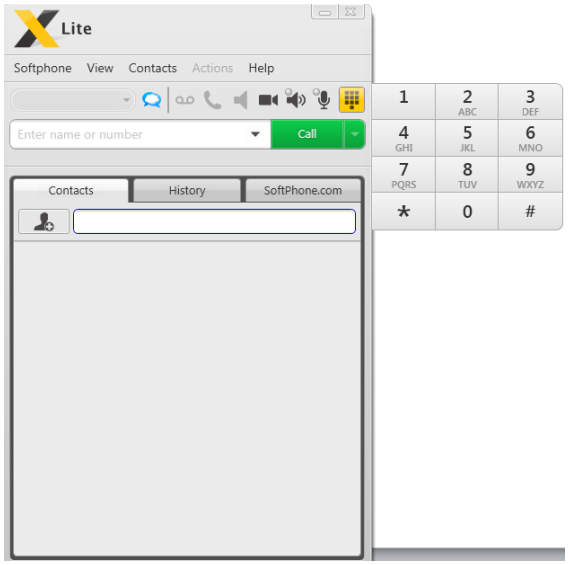


Gráfico Nº 6.50 X-Lite Conectado

Elaborado por: El investigador

6.8.4.1 Pruebas de conexión

Para comprobar que se estableció conexión y comunicación entre el sofphone y el servidor Asterisk a través de la VPN.

a) Ingresar en el servidor Asterisk a la CLI: /etc/Asterisk:

Ingresar a la CLI: Asterisk –rvvv

Y colocar el siguiente comando: sip show peers y va aparecer en la pantalla que el teléfono se registro con la IP que le asigno la VPN a la maquina remota, como se muestra en el Grafico 6.51

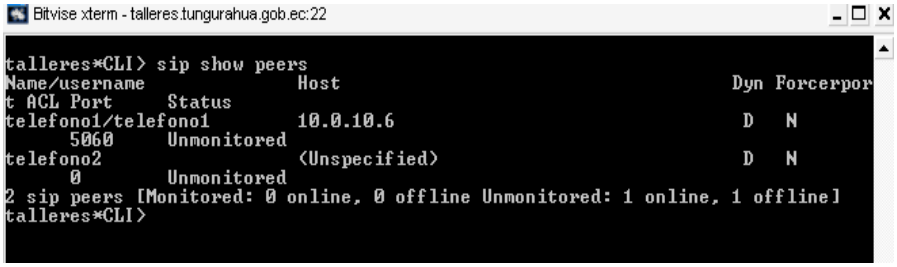


Gráfico Nº 6.51 Registro de teléfonos **Elaborado por:** El investigador

b) Realizando una llamada a las extensiones configuradas en el servidor Asterisk, se observa en la CLI los datos que se generan al llamar a la extensión

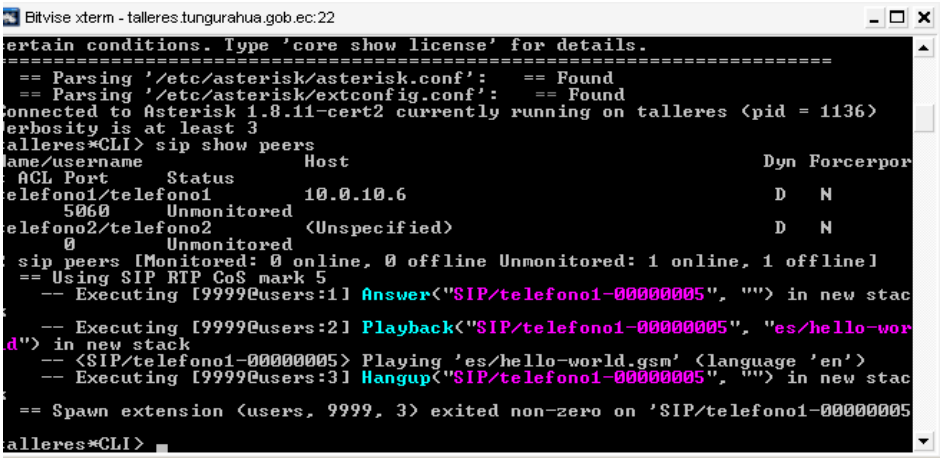


Gráfico Nº 6.52 Comprobación de comunicación

Elaborado por: El investigador

c) Llamando entre Sofphone X-Lite, como se muestra en el Grafico 6.53

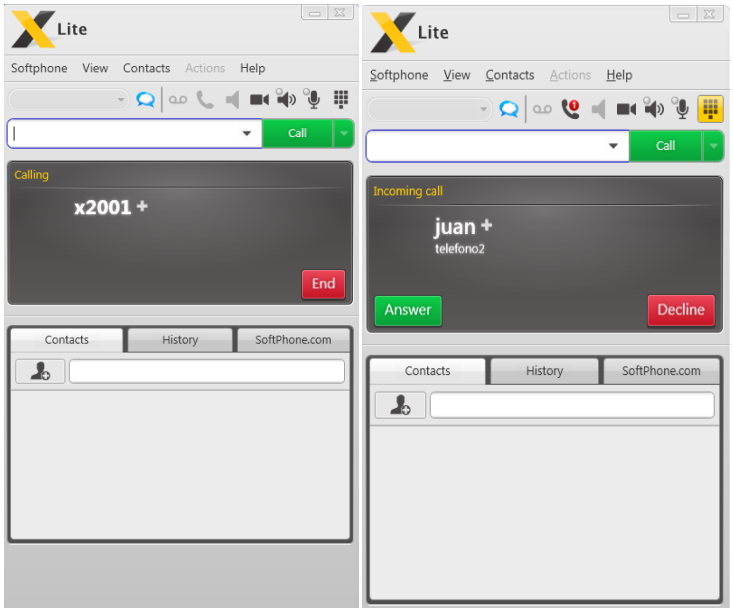


Gráfico Nº 6.53 Llamada entre 2 de X-Lite

Elaborado por: El investigador

6.8.5 Cálculos de envió de información Utilizando con Wireshark 1.6.8

Para el análisis del envió de información se utilizo el software WIRESHARK en el cliente VPN, ya que desde allí se enviara y se recibirá la información.

Primeramente con Wireshark hay analizar el flujo de datos que se genera al establecer la conexión como se muestra en el Grafico 6.54, se observa un panel de paquetes capturados, en este panel se despliega la lista de paquetes que se capturaron. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.

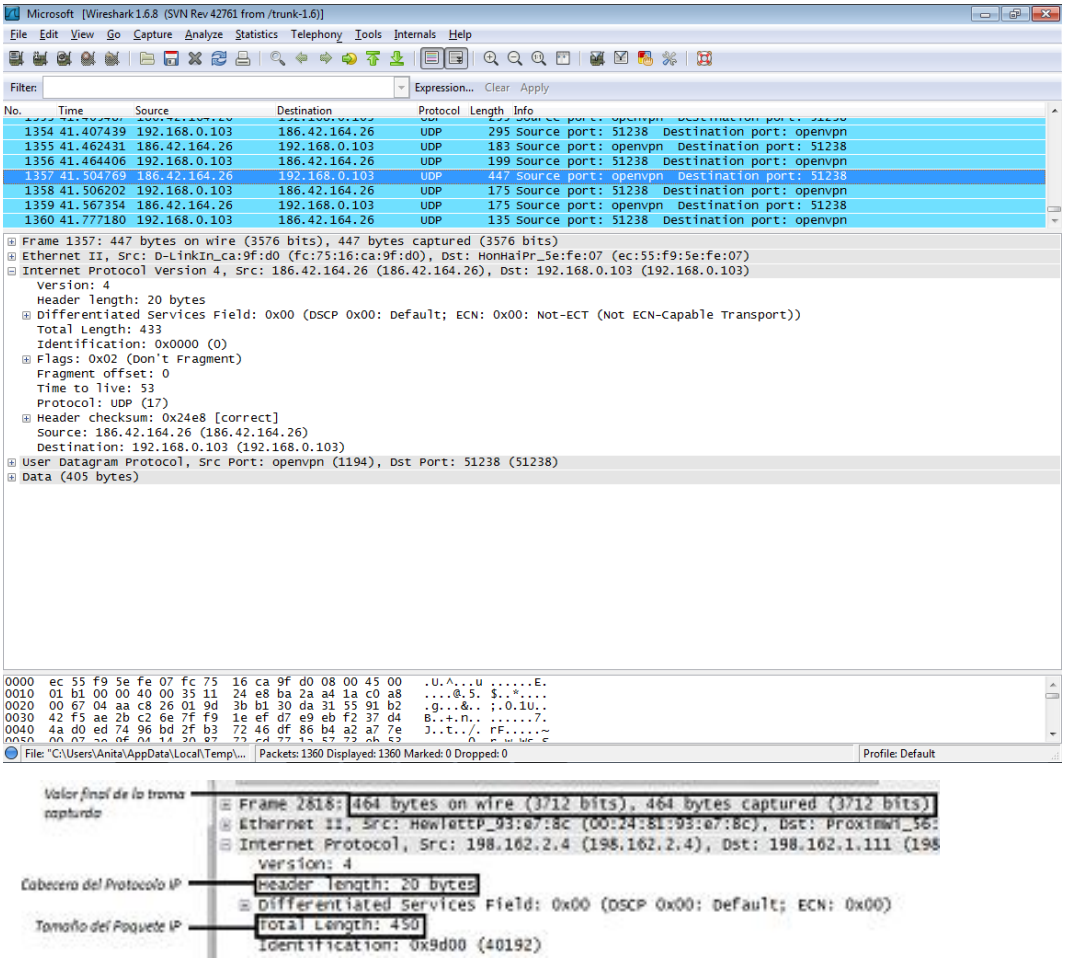


Gráfico Nº 6.54 Análisis Wireshark

Elaborado por: El investigador

Luego se selecciona la línea donde este la comunicación entre las 2 IPs (Servidor y Cliente) y hay que acceder al menú Statistics e ingresar en la opción Conversatios; este procedimiento se muestra en el Grafico 6.55.

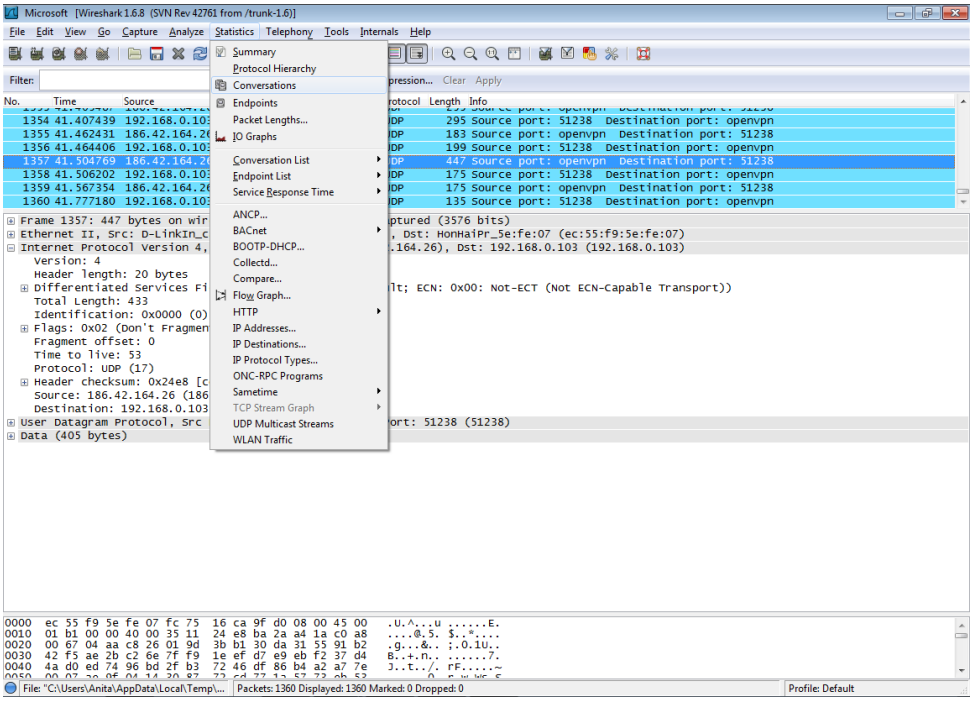


Gráfico Nº 6.55 Conversations

Elaborado por: El investigador

Esta opción permite distinguir varias conversaciones y también permite escoger el tipo de conversación que se desee analizar, en este caso tenemos que analizar UDP porque ese es el puerto utilizado tanto por el cliente como por el servidor donde se encuentra la aplicación. En el grafico 6.56 se puede visualizar el par de equipos a ser analizados.

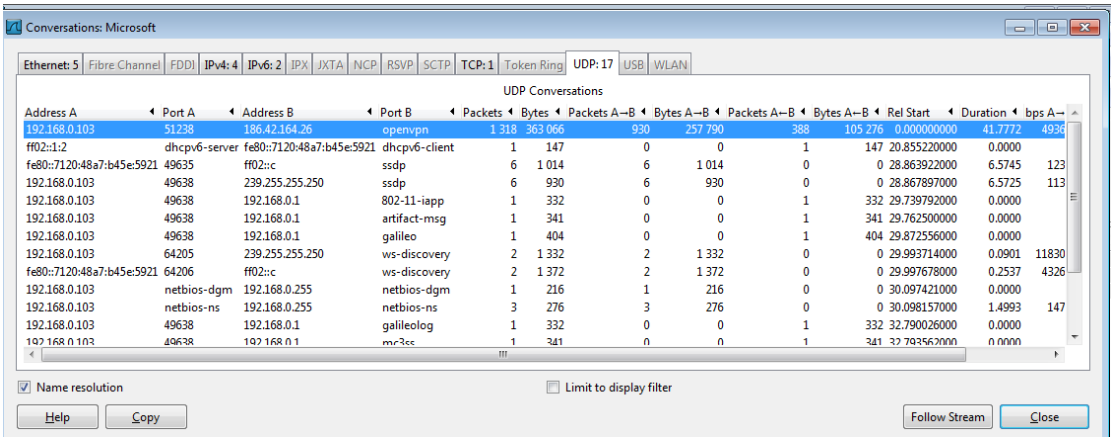


Gráfico Nº 6.56 Detalle de Conversations

Elaborado por: El investigador

Para el análisis se debe detallar los datos correspondientes a la conversación del cliente y el servidor Openvpn, en la tabla 6.1 se considera todos los aspectos requeridos para el dimensionamiento requerido

Tabla 6.1 Análisis de Transmisión de Información

Direccionamiento IP A	Direccionamiento IP B
192.168.0.103	186.42.164.26
PUERTO UDP A	PUERTO UDP B
51238	Openvpn
Paquetes	Paquetes
1318	1318
Bytes	Bytes
363066	363066
PAQUETES A->B	BYTES A->B
930	257790
PAQUETES A<-B	BYTES A<-B
388	105276
DURACION	DURACION
41,7772	41,7772
bps A->B	bps A<-B
49364.75	20159.52

Elaborado por: El investigador

Ahora hay que determinar la taza de transferencia del protocolo IP, para esto se debe obtener el número total de paquetes transferidos desde el Host cliente hacia el servidor y viceversa.

Paquetes transferidos = 1318

Ahora hay obtener el número total de bytes transferidos en la conversación:

Bytes transferidos = 363066
Tiempo total de conversación:

Tiempo = 41,7772 segundos

Se multiplica el valor de bytes de control Ethernet por el total de paquetes de la conversación:

Total Bytes Ethernet = Cabecera Ethernet * Paquetes transferidos
Total Bytes Ethernet = 20*1318
Total Bytes Ethernet = 26360

Restar el valor anterior (Total bytes Ethernet) del total de bytes transferidos:

Total bytes IP = Bytes transferidos-Total bytes Ethernet
Total bytes IP = 363066-26360
Total bytes IP =336706

Ahora el resultado de la operación anterior se divide para el tiempo total de conversación:

Ocupación del Canal = Total bytes IP / Tiempo de conversación
Ocupación del Canal = 336706 bytes / 41,7772 segundos
Ocupación del Canal = 8059,5635 bytes / segundos

El resultado encontrado en la operación anterior es la taza de transferencia hasta la capa de red que usa el protocolo IP; multiplicamos este valor por el número de bits que contiene un byte (8 bits).

Ocupación del Canal = 8059,5635 bytes / segundos * 8 bits
Ocupación del Canal = 64476,5087 bits/segundo / 1000
Ocupación del Canal = 64,4765 Kbps[27]

6.8.6 Conclusiones y Recomendaciones

Conclusiones

1) Luego del haber investigado acerca de una Conexión VPN se puede concluir que es una tecnología que nos permite transmitir cualquier tipo de información, en este caso voz y datos, objetivo primordial de este proyecto, con el cual los funcionarios del HGPT van a tener acceso a la información de las bodegas.

2) La administración de la red se facilita considerablemente, ya que el funcionamiento de esta red es muy sencilla y fácil de manejar, además esta depende del ancho de banda de Internet contratado.

3) En lo referente a costos, las VPNs configuradas por Software reducen considerablemente los egresos económicos en equipos de comunicación para la compartición de recursos entre dependencias que se encuentran distantes y que pertenecen a la misma organización, entonces se puede considerar que las Redes Privadas Virtuales son una alternativa ventajosa para cualquier organización.

[27] http://repo.uta.edu.ec/bitstream/handle/123456789/79/t601e.pdf?sequence=1

4) Al finalizar el presente proyecto sobre una Conexión VPN a través de Internet se puede concluir que todos los objetivos y metas propuestas se cumplieron satisfactoriamente, lo cual beneficio mucho al HGPT

Recomendaciones

1) Se recomienda a los administradores tener mucho cuidado con certificados y las claves de los usuarios ya que puede caer en malas manos y permitir el acceso a usuarios que no pertenecen a esta entidad, con esto se evita el plagio de datos importantes que le concierne solo a esta entidad.

2) Se debe renovar de manera periódica las claves y los certificados de los clientes, para así evitar que personas ajenas a la empresa ingresen a la red VPN

3) Es importante que se mejore el ancho de banda para que soporte el tráfico actual y el que será implementado una vez estén terminadas las bodegas, además se debe restringir el acceso a páginas que consuman demasiado ancho de banda como descargas, páginas sociales, juegos en línea, etc.

4) Se recomienda al departamento de sistemas del HGPT adquirir el servidor que sea específicamente para dar comunicación a través de la VPN.

6.9 Administración de la Propuesta

6.9.1 Aspecto Operativo

En cuanto al Aspecto Operativo para tener un buen funcionamiento de la Red Privada Virtual se recomienda cambiar y renovar los certificados digitales SSL/TLS y las claves de los usuarios continuamente en el servidor, así se podrá

evitar posibles ataques de intrusos externos sobre las red VPN, además proveer únicamente de los certificados y claves al personal encargado exclusivamente de la administración de la red

El correcto funcionamiento de la red se refleja en el ancho de banda utilizado en la conexión a internet tanto del servidor VPN como de los clientes, de eso depende que haya una comunicación eficiente.

6.9.2 Aspecto Económico

En cuanto a lo económico no hubo ningún gasto ya que los equipos utilizados forman parte del departamento de sistemas del HGPT.

Otro de los motivos es porque el proyecto en su totalidad tiene configuración en software.

BIBLIOGRAFÍA

- ✓ FIGUEIRAS, Aníbal. (2002) *Un Panorama De Las Telecomunicaciones*. Editorial Isabel Capella. España.

- ✓ Gil Pablo (2010). Redes y transmisión de datos, Primera Edición, Editorial Marfil

- ✓ Sanchis Enrique. (2004). Fundamentos y Electrónica de la Comunicaciones Volumen 72 de Educación (Universidad de Valencia) Editorial Colombiana.

- ✓ TOMASI, Wayne (1996). Sistemas de Comunicaciones Electrónicas. Primera edición. España. Editorial Prentice Hall.

LINKOGRAFIA

- ✓ Telecomunicaciones medios guiados y no guiados , Modificado el 21 de junio del 2001 http://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

- ✓ Red Inalámbrica publicada en febrero del 2006 http://es.kioskea.net/contents/wireless/wlintro.php3

- ✓ Grafica de los sistemas de comunicaciones http://html.rincondelvago.com/sistemas-de-comunicaciones.html

- ✓ Red privada virtual o VPN publicada en Septiembre del 2001 http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp

- ✓ Tecnología VPN publicado en mayo del 2009 http://tescoredes.wordpress.com/2011/05/29/

- ✓ Tipos Redes privadas virtuales publicado en febrero del 2005 http://blackspiral.org/docs/pfc/itis/node5.html , http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1875

- ✓ Protocolos de seguridad para redes privadas virtuales http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/doc/bmfcil732p.pdf

- ✓ Revista electrónica de estudios telemáticos, Acceso remoto de una VPN publicado por la universidad Rafael Belloso en junio del 2004 http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/doc/bmfcil732p.pdf

- ✓ Redes Privadas virtuales publicado en el 2009 delhttp://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/VPNgerardoBrollo.pdf

- ✓ Concepto general de Redes http://moncayo.unizar.es/ccuz/proced.nsf/0/5f94aec4f8aff02bc12569070046c1c1?OpenDocument

- ✓ VPN basadas en SSL/TLS http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

- ✓ Funcionamiento interno de SSL/TLS http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

- ✓ Openvpn http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

- ✓ Formas de Trabajo de Openvpn http://www.ecualug.org/2007/02/06/comos/centos/c_mo_instalar_y_configurar_openvpn
- ✓ Modo de Funcionamiento Openvpn

http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

- ✓ Asterisk
  http://linux.ctt-espe.edu.ec/12.pdf

- ✓ Recomendaciones de la ITU para VOIP
  http://www. repo.uta.edu.ec/handle/123456789/79

- ✓ Protocolos para Asterisk
  http://linux.ctt-espe.edu.ec/12.pdf

- ✓ Componentes de un Sistema Sip
  http://www. repo.uta.edu.ec/handle/123456789/79

- ✓ IAX, MGPC, H323
  http://linux.ctt-espe.edu.ec/12.pdf

- ✓ Stack de Protocolos H323, Direccionamiento, Señalización, Compresión de Voz, Transmisión de Voz, Control de Transmisión
  http://www.monografias.com/trabajos11/descripip/descripip.shtml

- ✓ Samba
  http://www.guia-ubuntu.org/index.php?title=Samba

- ✓ Descripción Server.conf y Cliente.conf
  http://www.comusoft.com/instalar-y-configurar-servicio-openvpn-en-servidor-y-cliente-linux

- ✓ Descripción Sip.conf y Extensions.conf
  http://www.voztele.com.mx/swf/MANUALES/Manual%20Asterisk%20Oigaa.pdf

TESIS

- ✓ Víctor Humberto Limari Ramírez Víctor Alberto (2004), Protocolos de seguridad de redes, UACH
- ✓ Lescano Felipe (2011), Tecnología Wireless para servicios de comunicación en zonas comerciales de Tungurahua, UTA
- ✓ Roberto Noé Molina Salas (2011), Red Privada Virtual (vpn) para la Transmisión de Servicios Multimedia sobre IP entre la Cooperativa de Ahorro y Crédito Ambato Ltda. y sus Sucursales, UTA
- ✓ Juan José Tomás Cánovas (2008), Servicio VPN de acceso remoto basado en SSL mediante OpenVPN, UNIVERSIDAD POLITÉCNICA DE CARTAGENA

GLOSARIO DE TERMINOS UTILIZADOS

HGPT = Honorable Gobierno Provincial de Tungurahua

PDU = Unidades de Datos de Protocolo, es un término que se utiliza para describir datos mientras se mueve de una capa a otra del modelo OSI.

JITTER= Variabilidad temporal durante el envío de señales digitales, una ligera desviación de la exactitud de la señal de reloj.

ADSL = Línea de abonado digital asimétrica, Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado.

SSL = (Secure Socket Layer) = Capa de conexión segura proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

TLS = (Transport Layer Security) =Seguridad de la capa de transporte, protocolo criptográfico que proporciona comunicación segura por una red.

TCP = Protocolo de Control de Transmisión, permite a dos anfitriones establecer una conexión e intercambiar datos. Es un protocolo de comunicación orientado a conexión de nivel de transporte. Es un protocolo de capa 4 según el modelo OSI.

HTTP = Protocolo de Transferencia de Hipertexto, define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web.

FTP = Protocolo de Transferencia de Archivos, el servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.

SMTP =Protocolo Simple de Transferencia de Correo, protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

Telnet = Telecommunication Network, es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet.

DES = Estándar de Cifrado de Datos, es un algoritmo de cifrado,

AES = Estándar de Cifrado Avanzado.

MAC = Código de autenticación de Mensaje, es una porción de información utilizada para autenticar un mensaje.

MD5 = Algoritmo de Resumen del Mensaje.

SHA-1 = Algoritmo de Hash Seguro, ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo.

HTTPS = Protocolo de Transferencia de Hipertexto Seguro

GPL = Licencia General Publica, está orientada principalmente a proteger la libre distribución, modificación y uso de software.

IPSec = Protocolo de seguridad de Internet, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet(IP) autenticando y/o cifrando cada paquete IP en un flujo de datos

OSI = Modelo de Interconexión de Sistemas Abiertos, el modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes

IKE = Intercambio de Claves de seguridad, es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPsec.

PPTP = Protocolo de Tunel Punto a Punto, permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual.

VPN = Red Privada Virtual.

KERNEL = El kernel ó núcleo de linux se puede definir como el corazón de este sistema operativo. Es el encargado de que el software y el hardware de un ordenador puedan trabajar juntos.

UDP = Protocolo de Datagrama de Usuario, es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI).

TUN = Modo Túnel

TAP = Modo Puente

IP = Potolo de Internet, es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías.

Ethernet = Tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.

IPX = Intercambio de Paquetes Interred, es un protocolo de la capa de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

IANA = La Autoridad de Asignación de Números de Internet, es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. Actualmente es un departamento operado por ICANN.

DOS = Sistema Operativo de Disco, contaba con una interfaz de línea de comandos en modo texto o alfanumérico.

RTP = Protocolo de Transporte de Tiempo Real, Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

VoIP = Voz sobre Protocolo de Internet es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP.

PBX = Private Branch Exchange, se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior.

PSTN = Red Telefónica Pública Conmutada, es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real.

FXO = Es un dispositivo de computador que permite conectar éste a la RTB, y mediante un software especial, realizar y recibir llamadas de teléfono.

URA = Unidad de Respuesta Audible, En general es un PC convencional, que se añade un hardware específico para realizar las tareas de la telefonía (por ejemplo, responder, marcar, apagado, el reconocimiento de dígitos, hablar, etc).

DAC = Conversión Digital a Análogo.

GSM = Sistema Global para las Comunicaciones Móviles.

SIP = Protocolo de Inicio de Sesiones.

G.711 = Es un estándar para representar señales de audio con frecuencias de la voz humana, mediante muestras comprimidas de una señal de audio digitalcon una tasa de muestreo de 8000 muestras por segundo.

RTCP = Protocolo de Control en Tiempo Real, es un protocolo de comunicación que proporciona información de control que está asociado con un flujo de datos para una aplicación multimedia.

IAX = Inter-Asterisk eXchange protocol, es uno de los protocolos utilizado por Asterisk, un servidor PBX (central telefónica) de código abierto

MGCP = Media Gateway Control Protocol, es un protocolo interno de VoIP cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente – servidor.

POST = Servicio Telefónico Ordinario Antiguo (conocido también como Servicio Telefónico Tradicional o Telefonía Básica), se refiere a la manera en como se ofrece el servicio telefónico analógico (o convencional) por medio de cableado de cobre.

PCM = Modulación por Impulsos Codificados, es un procedimiento de modulación utilizado para transformar una señal analógica en una secuencia de bits

Cisco SCCP = Skinny Client Control Protocol, se define como un conjunto de mensajes entre un cliente ligero y el CallManager.

ALSA = Advanced Linux Sound Architecture, módulo de Arquitectura de Sonido Avanzada para Linux.

NAT = Traducción de Dirección de Red, es un mecanismo utilizado por encaminadores IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

IETF = Grupo Especial sobre Ingeniería de Internet, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

Q.931 = Es un protocolo de señalización que contiene funciones de establecimiento y desconexión.

SMB = Es un Protocolo de red que pertenece a la capa de aplicación en el modelo OSI que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red.

CIFS = Versión Actualizada de SMB incluyen soporte para enlaces simbólicos, enlaces duros (hard links), y mayores tamaños de archivo.

SSH = Secure Shell, es un protocolo que acceder a máquinas remotas a través de una red o a través de internet.

Debían = Es una comunidad conformada por desarrolladores yusuarios, que mantiene un sistema operativo GNU basado en software libre.

ANEXOS

Anexo A

DESCARGA E INSTALACIÓN DE TUNNELIER

Tunnelier permite emular los protocolos bvterm, xterm y vt100, establecer conexiones de FTP a SFTP, y es capaz de realizar forwading a traves de Proxy y SOCKS. Incluye funciones de reconexion administracion remota de WinSSHD.
Para descargar Tunnelier ingresamos a la página de tunelier a la parte de descargas, con el siguiente link http://www.bitvise.com/download-area
Y le damos en la primera opción: Download Bitvise SSH Client, luego en la opción Bitvise SSH Client installer.

Una vez descargado procedemos a instalar, aceptando los términos e instalando todas las dependencias.

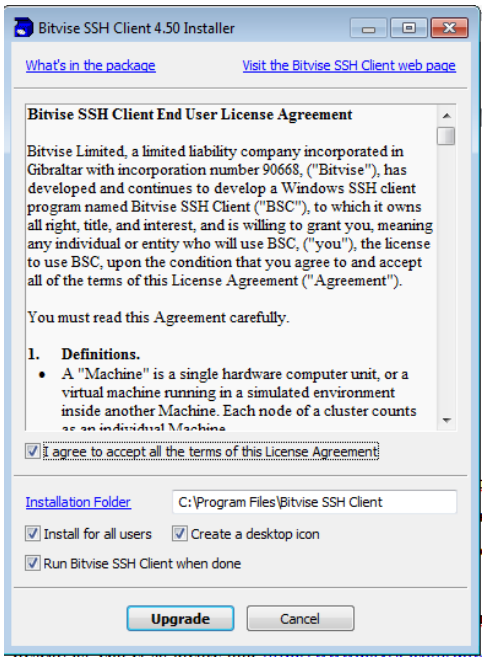


Gráfico Nº A.1 Instalación Tunnelier
Elaborado por: El investigador

Cuando esté instalado saldrá una ventana como la que se muestra en el siguiente grafico.

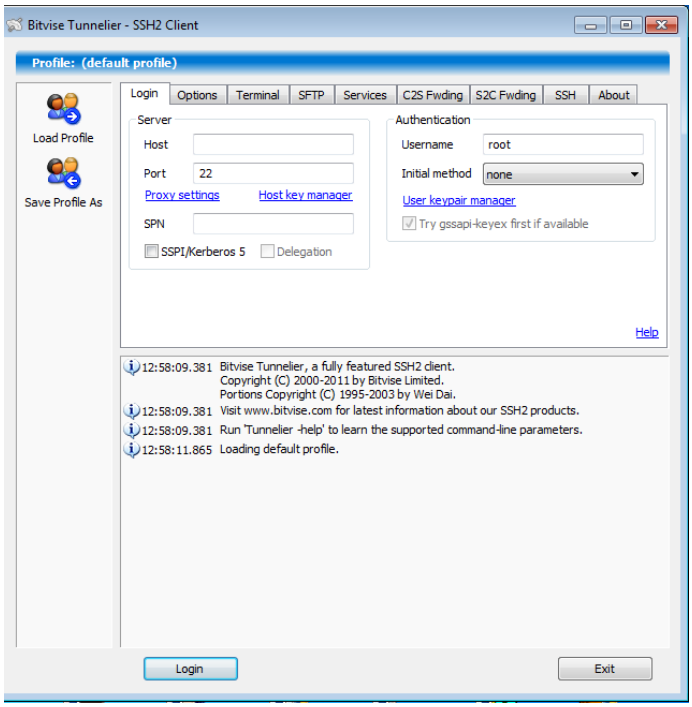


Gráfico Nº A.2 Ventana Principal de Tunnelier

Elaborado por: El investigador

Aquí ingresamos los datos del servidor al cual queremos conectarnos.:

Host = Dirección o DNS del servidor

Port = Puerto por el cual se va a Conectar

Username = Nombre con el Cual ingresa a la Consola del Servidor

Initial method = Metodo de ingreso, lo más común es por medio de un password.

Login = Una vez que los datos estén correctos ingresamos al servidor.

Anexo B

DESCARGA E INSTALACIÓN DE OPENVPN EN WINDOWS 7

En primer lugar, es necesario descargar el cliente OpenVPN GUI desde http://openvpn.net/index.php/open-source/downloads.html la ultima versión de openvpn es openvpn-2.2.2-install.exe

Instalación del cliente es muy sencilla, sólo confirmar las opciones por defecto es suficiente.
Después de descargar el archivo antes mencionado, hacemos clic sobre él, se iniciará el proceso de instalación. Al hacer clic en Siguiente le llevará a la ventana de configuración inicial.

Gráfico Nº B.1 Instalación Openvpn 2.2.2
Elaborado por: El investigador

A continuación aparecerán los términos y condiciones para el uso del programa. Seleccionamos la opción *I agree* y hacemos un click en *Next* para aceptar los terminos.

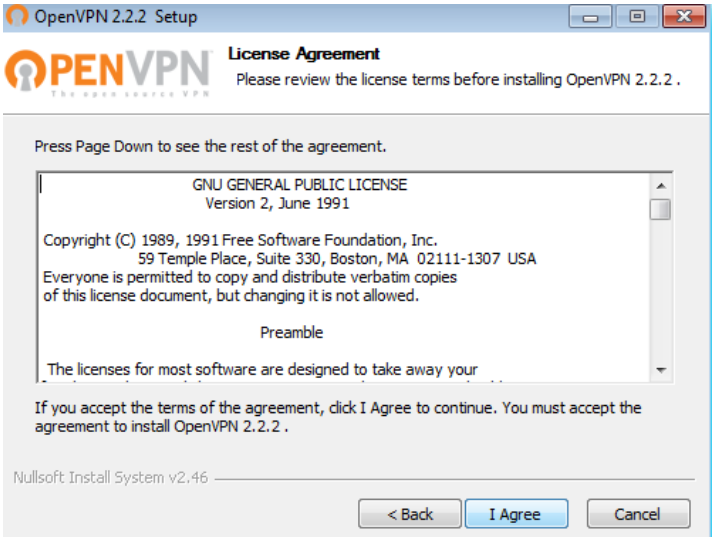


Gráfico Nº B.2 Licencia Openvpn 2.2.2

Elaborado por: El investigador

En la siguiente ventana hay que dejar los valores predeterminados.

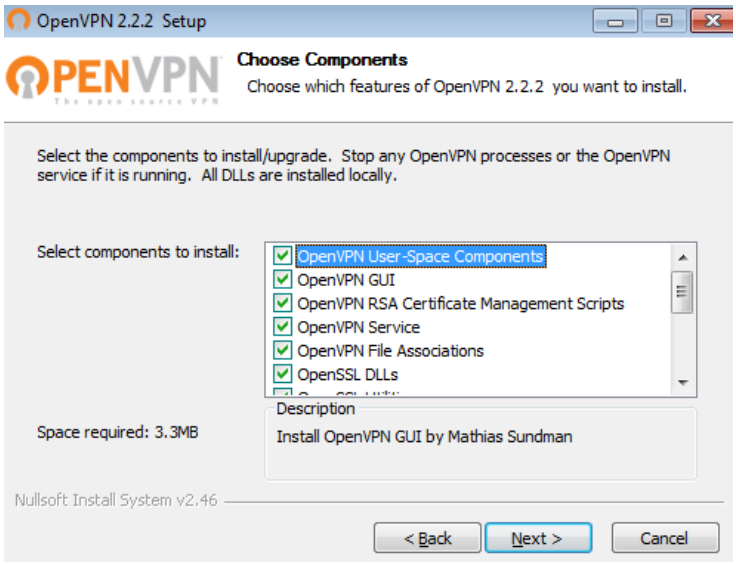


Gráfico Nº B.3 Componentes Openvpn 2.2.2

Elaborado por: El investigador

Damos click en Next, Install, Next, y una vez que la instalación se complete damos click en finalizar, y Openvpn estará instalado en el Sistema Operativo Windows 7.

Anexo C

CONFIGURACIÓN DEL FIREWALL DE UBUNTU 12.04 MEDIANTE WEBMIN

Para un mejor entendimiento y facilidad de configuración del firewall, se instalo la herramienta Webmin.

Webmin es una herramienta de configuración de sistemas accesible vía web para OpenSolaris, GNU/Linux y otros sistemas Unix. Con él se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etcétera, así como modificar y controlar muchas aplicaciones libres, como el servidor web Apache, PHP, MySQL, DNS, Samba,DHCP, entre otros

Primero descargamos r instalamos Webmin en el servidor Ubuntu 12.04 con el comando

wget http://prdownloads.sourceforge.net/webadmin/webmin_1.580_all.deb y dpkg -i webmin_1.580_all.deb

Después saldrá una falla, es ahí cuando colocamos el comando **apt-get install –f** con lo cual se va a instalar todas la dependencias necesarias para la instalación.

Una vez instalado podemos acceder a la interfaz web de Webmin usando un navegador y escribiendo la dirección IP del equipo donde está instalado seguida del puerto donde está escuchando, por defecto, el 10.000. Eso sí, debemos estar atentos porque en vez de usar el protocolo HTTP, usaremos el HTTPS.

Va a salir una advertencia que no es un sitio de confianza, damos click en Continuar de todos modos.

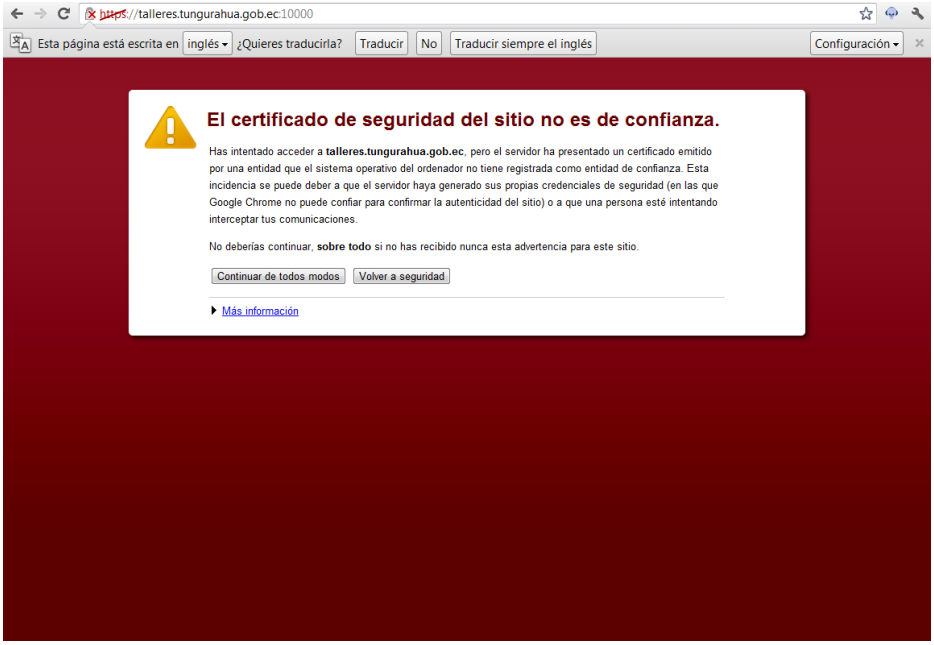


Gráfico Nº C.1 Dominio Webmin

Elaborado por: El investigador

Ahora ya podemos iniciar sesión en Webmin. Como nombre de usuario podemos usar root (si lo tenemos habilitado) o cualquier usuario del sistema con privilegios de administrador

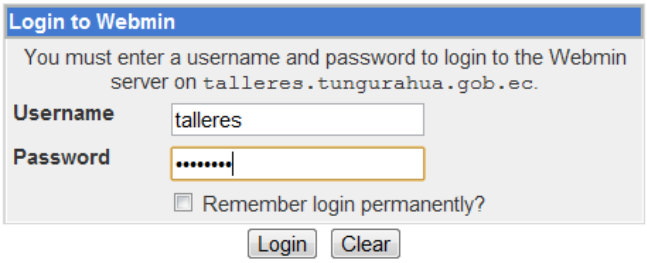


Gráfico Nº C.2 Login Webmin

Elaborado por: El investigador

Una vez dentro vamos a la pestaña que dice Red, luego a Cortafuegos Linux.

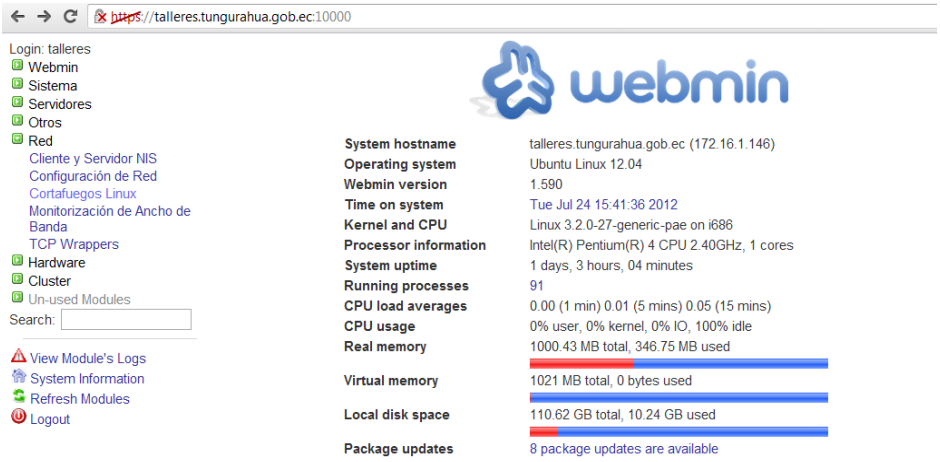


Gráfico Nº C.3 Interfaz de Webmin

Elaborado por: El investigador

En el cortafuegos de Linux nos vamos a dar cuanta que hay tres secciones l primera dice *Paquetes entrantes (INPUT),* la segunda *Paquetes redirigidos (FORWARD),* y la tercera *Paquetes salientes (OUTPUT).*

Ingresamos en Paquetes Entrantes y configuramos los siguientes puntos

Acción a ejecutar= Aceptar

Dirección o Red de destino= La dirección publica del Servidor si no la tiene Dirección local del Servidor (dirección privada)

Protocolo de Red = Igual a, protocolo que se utilice para la aplicación en nuestro caso UDP

Puerto TCP o UDP Destino = Igual a, protocolo utilizado en la aplicación, en nuestro caso utilizamos el puerto 1194, 7098, 9078

Tipo de paquete ICMP = en nuestro caso any (cualquiera)

Guardamos

De igual manera en la pestaña Paquete redirigidos colocamos la misma configuración,

Acción a ejecutar= Aceptar

Dirección o Red de destino= La dirección publica del Servidor si no la tiene Dirección local del Servidor (dirección privada)

Protocolo de Red = Igual a, protocolo que se utilice para la aplicación en nuestro caso UDP

Puerto TCP o UDP Destino = Igual a, protocolo utilizado en la aplicación, en nuestro caso utilizamos el puerto 1194, 7098, 9078

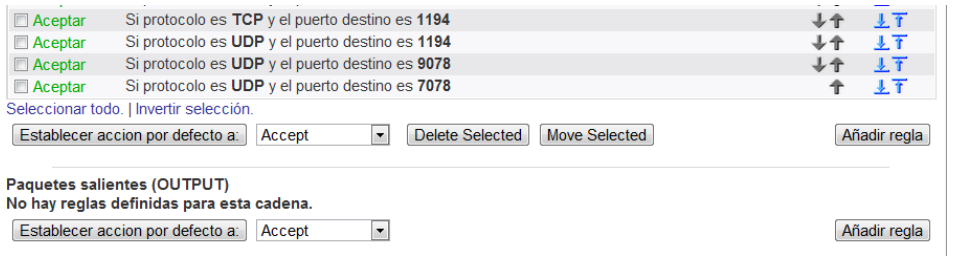
Tipo de paquete ICMP = en nuestro caso any (cualquiera)

Guardamos

Como la empresa tenía configurada una NAT para la dirección del servidor la configuración queda de la siguiente manera.

Input

Forward



Postrouting

Gráfico Nº C.4 Configuración del Firewall mediante Webmin

Elaborado por: El investigador

Anexo D

DESCARGA E INSTALACION DEL SOFPHONE X-LITE

El sofphone que se utilizo es X-Lite. Esta aplicación la descargamos del siguiente Link: http://www.counterpath.com/x-lite-download.html

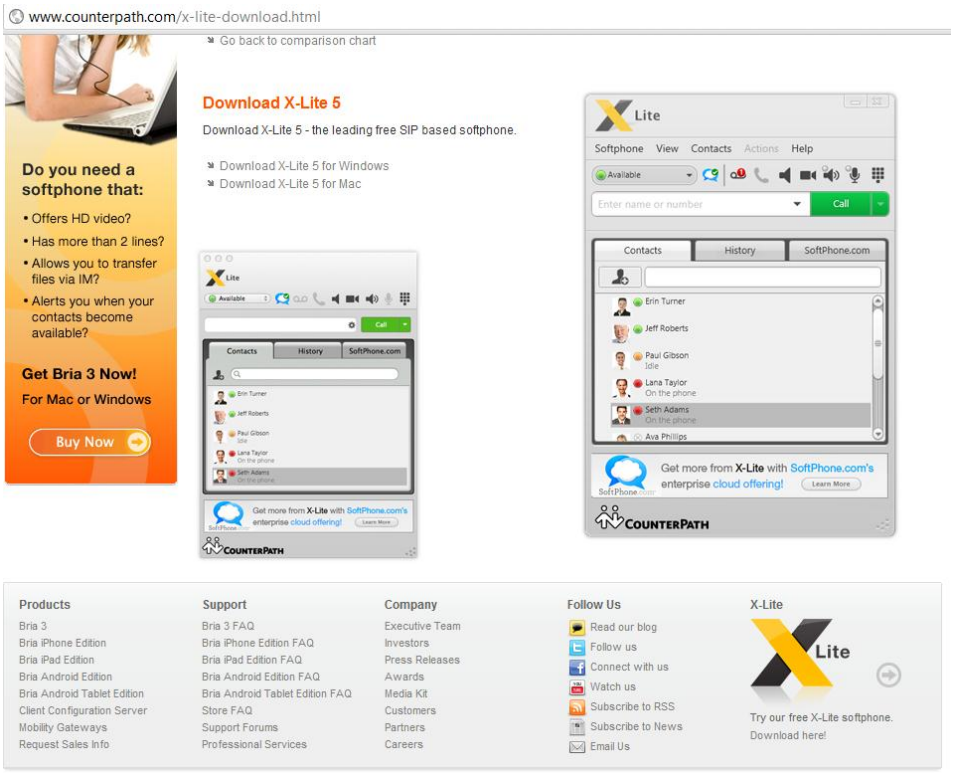


Gráfico Nº D.1 Pagina de descarga X-Lite

Elaborado por: El investigador

Ya descargado X-Lite en el computador lo ejecutamos. Al aparecer la Pantalla de bienvenida le damos click en el botón Next.

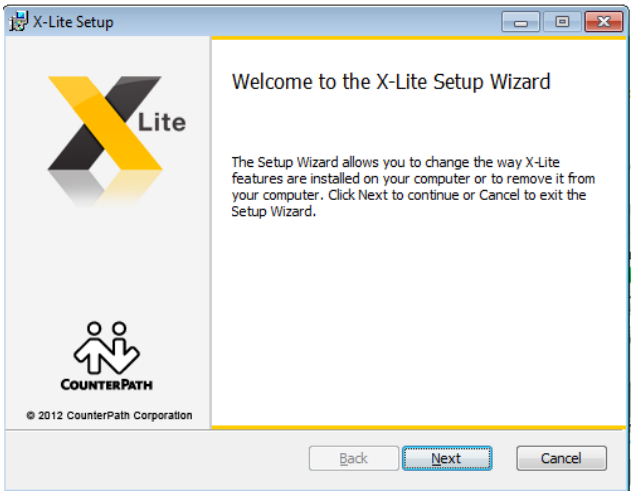


Gráfico Nº D.2 Pantalla Bienvenida X-Lite

Elaborado por: El investigador

A continuación aparecerán los términos y condiciones para el uso del programa. Seleccionamos la opción *I accept the terms in the Licence Agreement* y hacemos un click en *Next* para aceptar los terminos.

Gráfico Nº D.3 Términos y Condiciones X-Lite

Elaborado por: El investigador

Opcionalmente se puede cambiar el directorio donde se instalará el programa. En caso no se necesita cambiarlo, hacemos click directamente en Next para continuar, luego también Next.

Una vez realizados los pasos anteriores, aparecerá una ventana en donde se debe confirmar la instalación con el botón Install. Y el programa comenzará a instalarse.

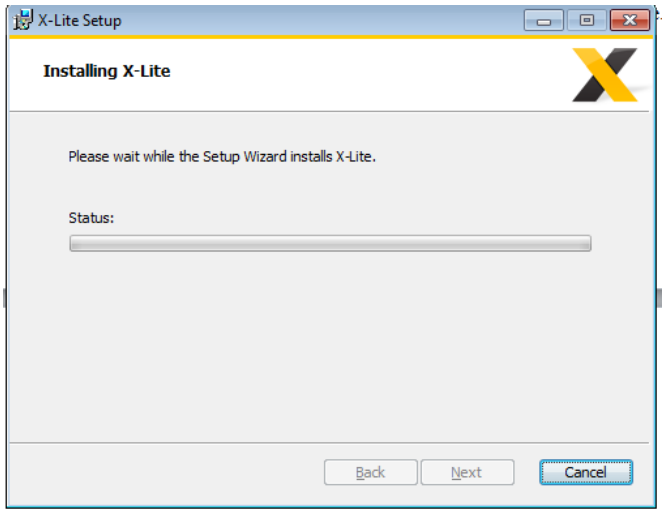


Gráfico Nº D.4 Instalación X-Lite

Elaborado por: El investigador

Una vez finalizado el proceso de instalación, hacemos click en Finish para terminar la instalación.

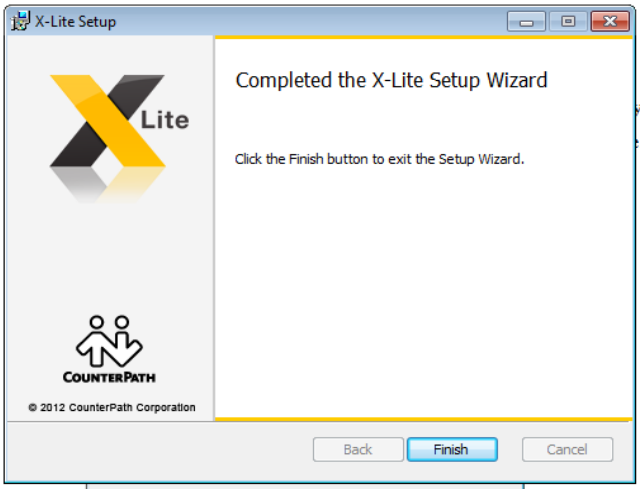


Gráfico Nº D.5 Instalación Finalizada

Elaborado por: El investigador

Anexo E

SERVER.CONF, CLIENT.OVPN, SIP.CONF Y EXTENSIÓN.CONF

Server.conf

Dispositivo Tunel.

dev tun

Usar protocolo TCP en el Puerto 1194

proto tcp

port 1194

Configuración de parámetros SSL

ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt

cert /etc/openvpn/easy-rsa/2.0/keys/server.crt

key /etc/openvpn/easy-rsa/2.0/keys/server.key

dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem

Usuario y grupo para identificarse en el protocol smb

user nobody

group nogroup

Dirección de red y mascara que se usará en el túnel OpenVPN

server 192.168.67.0 255.255.255.0

Mantener las claves y la configuración después de reiniciar

persist-key

persist-tun

Permitir comunicación entre clientes

client-to-client

Permitir que varios clients usen la misma llave

duplicate-cn

Enrutar el cliente a una red local a la cual esté conectada el servidor.

push “route 192.168.1.0 255.255.255.0″

Comprimir la información antes de enviar por el tunel

comp-lzo

Descripción de los archivos de configuración client.ovpn

Client.ovpn

Especificar que este archive pertenece a un Cliente.

client

Usar una interfaz de tunel.

dev tun

Usar el protocol TCP

proto tcp

Especificar la ip o hostname del servidor y el puerto

remote ju4ns3.hopto.org 1194

hacer intentos de conexión infinitos.

resolv-retry infinite

no escuchar en ningún Puerto.

nobind

Nombre de usuario y grupo que se usarán para compartir recursos con sistemas Windows

user nobody

group nogroup

Mantener la clave y el tunel aun después de reiniciar.

persist-key

persist-tun

Definir parámetros SSL acá se ponen las rutas de los archivos correspondientes a las llaves.

ca ca.crt

cert client1.crt

key client1.key

Asignar el tipo de certificado

ns-cert-type server

Habilitar la compresión

comp-lzo

Nivel de detalle del log

verb 3[28]

Descripción de cada uno de los parámetros de la configuración sip.conf

Sip.conf

```
[general]                          ; En primer lugar existe la sección [general],
                                   ; donde se definen variables globales y
                                   aspectos
                                   ; por defecto para todos los canales SIP.
context=default ;                  ; Contexto por defecto donde entraran las
                                   ; llamadas entrantes por SIP.
                                   ; Este contexto se define en extensions.conf
localnet = 192.168.1.0/255.255.255.0
                                   ; debe especificar la dirección de su red, no la
                                   ; del equipo, y la correspondiente máscara
                                   ; siguiendo direccionamiento de tipo privado
bindport=5062                      ; puerto UDP al que hacer el bind
disallow=all                       ; deshabilitar todos los codecs
                                   ; habilitar codecs en orden de preferencia
allow=g729                         ; permitir el codec g729 (si se dispone de la
                                   ; licencia)
allow=alaw                         ; permitir el codec g711a
allow=ulaw                         ; permitir el codec g711u
canreinvite=no                     ; típicamente 'no' si se encuentra detrás de un
                                   ; NAT.
                                   ; De este modo se habilita que el tráfico RTP
                                   ; (voz) pase por el sistema Asterisk.
nat=yes                            ; Cuando nos encontramos detrás de un NAT.
                                   ; Si aparecen problemas de audio, en solo un
                                   ; sentido, pueden ser originados por la
                                   ; configuración NAT de su firewall/router y el
```

[28] http://www.comusoft.com/instalar-y-configurar-servicio-openvpn-en-servidor-y-cliente-linux

```
                                ; soporte para puertos SIP y RTP. Puede
                                ; definir los puertos RTP para audio entrante
                                ; en el archivo rtp.conf del sistema Asterisk
dtmfmode=rfc2833                ; Permite especificar el método por el cual se
                                ; enviaran los tonos (dígitos pulsados durante
                                la
                                ; conversación).
                                ; rfc2833 para mandar los tonos DTMF como
                                ; RTP
                                ; username: usuario asignado por Vo
                                ztelecom
                                ; password: contraseña asignada por
                                Voztelecom
defaultexpirey=30               ; definimos el expire

[1000]                          ; Configuramos el cliente.
                                ; Se ha definido la extensión 1000 para poder
                                ; realizar funciones básicas de test de la
                                ; instalación e interconexión con el Servidor.
type=friend                     ; friend= configuración peer + user
                                ; Dispositivo que puede tanto recibir como
                                ; realizar llamadas a través del sistema
                                Asterisk
regexten=1000
host=dynamic                ;Habilitamos que el teléfono se pueda registrar
                                ; desde cualquier ip


secret=1000                     ; Define el password para la extensión,
                                ; debe ser una cadena de tipo alfanumérico
nat=no                          ; No hay nat entre el dispositivo y el sistema
                                ; Asterisk
```

```
[from-voztelecom]          ; Para recibir llamadas del host sip.mx.voztele.com
type=friend                ; friend= configuración peer + user,
                           ; dispositivo que puede tanto recibir como
                           ; realizar llamadas a través del sistema Asterisk
host=sip.voztele.com.mx      ;definimos el host de Voztelecom
context=incoming           ; tal y como lo definimos en extensions.conf
```

Descripción de los parámetros del archivo de configuración extensions.conf

Extensions.conf

```
[general]                                  ; Definición del contexto general
static=yes
writeprotect=no                            ; con static=yes y writeprotect=no se habilita
                                           ; salvar un plan de marcado a través del
                                           ; comando CLI 'save dialplan'
autofallthrough=yes                        ; al finalizar las tareas Asterisk finalizará la
                                           ; llamada con BUSY, CONGESTION o HANGUP
clearglobalvars=no                         ; variables globales persistentes
priorityjumping=no

[globals]                                  ; En globals se pueden definir las variables
                                           ;globales que pueden usarse posteriormente en
                                           ; las extensiones. Una variable global se define
                                           ; del siguiente modo:
                                           ; nombre_de_la_variable => valor_de_la_variable
CONSOLE=Console/dsp                        ; Console interface
[default]                                  ; extension , priority , application
exten => _0.,1,Answer                      ; Acepta la llamada entrante por el canal
exten => _0.,2,Dial(SIP/${EXTEN:1}@voztelecom,30
                                           ; La aplicación Dial realiza una
```

```
                                ; llamada a un determinado destino,
                                ; si el destino acepta la llamada,
                                ; Asterisk conecta el origen primario
                                ; de la llamada con este nuevo interlocutor.
exten => _0.,3,Hangup           ; Cuelga la llamada
[incoming]                      ; Contexto que indica que hacer con
                                ; todas las llamadas entrantes
                                ; alias_pstn: número de teléfono
                                ; asignado
exten => <alias_pstn>,1,Answer  ; Acepta la llamada entrante por el ca
                                ;canal
exten => <alias_pstn>,2,Dial(SIP/1000)  ; Dirigir la llamada hacia la 1000
                                        ; ext.1000
exten => <alias_pstn>,3,Hangup          ; Cuelga la llamada[29]
```

[29] http://www.voztele.com.mx/swf/MANUALES/Manual%20Asterisk%20Oigaa.pdf

Anexo F

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Observación y Entrevista dirigida al departamento de sistemas del H. GOBIERNO PROVINCIAL DE TUNGURAHUA

OBJETIVO: Recolectar información sobre la actual condición de las comunicaciones entre las bodegas del H. GOBIERNO PROVINCIAL Y SU EDIFICIO PRINCIPAL.

Entrevista dirigida al administrador del departamento de sistemas del HGPT Nº 1

¿En qué estado se encuentran los equipos de comunicación del departamento de sistemas del H.G.P.T?

Nº	Tipo	Cant.	Nombre	Descripcion	Rendimiento

Servicio	Servidor	Plataforma Servidor	Plataforma Clientes

Entrevista dirigida al administrador del departamento de sistemas del HGPT Nº2

¿Posee Ancho de banda necesario para abastecer su sistema de comunicación?

Entrevista dirigida al administrador del departamento de sistemas del HGPT Nº3

¿Qué Beneficios traerá la implementación de la Conexión VPN?

Entrevista dirigida al administrador del departamento de sistemas del HGPT Nº4

¿Cuál es el nivel de conocimiento del personal del departamento de sistemas para administración de una VPN?

Observación Nº1

Tecnología con la que cuenta el edificio central para la transmisión de información con sus bodegas

Tipo de tecnología	Velocidad de Trasmisión

Observación Nº2

Protocolos de comunicación que se utiliza en la conexión con las bodegas´

Protocolos	Capa

Observación Nº3

Eficiencia de la conexión que existe entre el edificio central y las bodegas del H.G.P.T

Observación Nº4

Nivel de seguridad de los sistemas de comunicación del departamento de sistemas del H.G.P.T para él envió y recepción de información

Servicio	Servidor	Plataforma Servidor

No.	Nombre	Descripción	Sis. Operativo	Aplicaciones