GOBIERNO DEL ESTADO DE CHIAPAS
SECRETARÍA DE EDUCACIÓN
SUBSECRETARÍA DE EDUCACION ESTATAL
DIRECCION DE EDUCACION SUPERIOR
DEPARTAMENTO DE SERVICIOS ESCOLARES Y BECAS
UNIVERSIDAD LINDA VISTA
INGENIERÍA EN SISTEMAS COMPUTACIONALES
CLAVE 000000

CURSO DE TITULACIÓN

REDES PRIVADAS VIRTUALES

PRESENTA

ALDRIN ISRAEL GÓMEZ ESTRADA

PARA OBTENER EL TÍTULO DE
INGENIERO EN SISTEMAS COMPUTACIONALES

PUEBLO NUEVO SOLISTAHUACÁN, CHIAPAS, NOVIEMBRE DE 2013.

TABLA DE CONTENIDO

LISTA DE FIGURAS

RECONOCIMIENTOS

A Dios primeramente que me ha preservado la vida hasta estos momentos. A mis padres que siempre me han apoyado en mi vida. Sé que hoy soy lo que soy gracias a ellos. A mis hermanos que siempre han estado en los buenos y sobre todos en los malos momentos.

CAPÍTULO I

INTRODUCCIÓN Y PLANTEAMIENTO DEL PROBLEMA

Introducción

La característica principal del periodo en el que vivimos es la creación e implementación de diferentes tecnologías de la información. La necesidad de las diferentes corporaciones motivan la creación de redes LAN, WAN, intranet, extranet y claro, el Internet. Las empresas conectan sus sucursales con la oficina central a través de redes WAN. También se puede instalar infraestructura para permitir el acceso remoto. Pero surge una problemática al tratar de mantener una red privada en estas condiciones: resulta ser en la mayoría de las ocasiones costosa y poco segura. Una red pública como Internet esta infestada de usuarios malintencionados, un sistema se vuelve inseguro simplemente con el mero hecho de encenderlo. El único sistema totalmente seguro sería uno que estuviese apagado, desconectado de cualquier red, metido dentro de una caja fuerte de titanio, rodeado de gas y vigilado por unos guardias armados insobornables. Aún así yo no apostaría mi vida por él "(Gene Spafford), experto en seguridad. Así que se requiere de una tecnología que permita el envío seguro y confidencial de los datos a través de una red pública como las VPN (redes privadas virtuales por sus siglas en inglès). La presente memoria pretende analizar el modo en el que la Uni-

versidad Linda Vista podría implementar esta tecnología en sus sede y campus, para ahorrar costos y evitar pérdida de datos importantes al momento de hacer transacciones. Las VPN están cobrando fuerza cada día en las empresas e instituciones de gobierno y educativas ya que ofrecen una variedad de ventajas. La seguridad es el aspecto principal de las VPN ya se trata de la información privada de las empresas circulando a través de Internet, es necesario entonces el uso de métodos de encriptacion y autenticacion de los datos con el fin de lograr el envío seguro de la información.

La estructuracion de dicho trabajo consiste en 3 capitulos. el primero de ellos consta de los sigientes pasos:

introducción, declaración del problema, delimitación, definición de términos.

El segundo es el marco teorico y se compone de las siguientes secciones: redes privadas virtuales, componentes de una VPN, VoIP, Sistema Operativo.

El capitulo 3 consta de la propuesta y esta constituido de las siguientes secciones: diseño, diagramas, costos, cerrando dicho proyecto de investigación con la conclusión .

Declaración del Problema

La mayoría de las empresas, institutos, universidades, etc., requieren métodos para poder transmitir información de la manera más rápida, segura, y a un precio razonable. Esto ha llevada a la necesidad de crear e implementar nuevas tecnologías al fin de satisfacer las necesidades latentes de las organizaciones en este mundo globalizado. En la actualidad la Universidad Linda Vista tiene un alto gasto en llamadas

telefónicas hacia los otros campus, inseguridad al momento de enviar información delicada, así como la limitación de estar dentro del campus para poder trabajar de una manera rápida y correcta. Es por eso que en la realización de esta investigación se pretende resolver la siguiente interrogante ¿Cuáles son los beneficios que ofrecen las redes privadas virtuales en la Universidad Linda Vista para el manejo de la información de todos sus campus? ¿Es factible intalar servicio de VoIP en las oficinas de la administracion de la Universidad Linda Vista?

Objetivos

Objetivo General. Conocer el impacto que tienen las redes privadas virtuales en la Universidad Linda Vista incluyendo sus campus (Tuxtla Gutierrez, Chiapas), en cuanto a costos y tiempo.

Objetivos Específicos.

1. Diseñar una red privada virtual para la Universidad Linda Vista.
2. Diseñar un servidor VoIP para llamadas telefonicas.
3. Estudiar casos de éxito en otras empresas que ya utilizan esta tecnología.

Justificación

Una red privada virtual podría favorecer el flujo de información de la Universidad Linda Vista el cual impactara en la reducción de costo. ya que en la actualidad los medios de información que se utilizan son: teléfono, correo electrónico, Internet. Los efectos que se esperan al implementar esta tecnología son reducción de costos al

momento de comunicarse con los distintos campus, mayor seguridad al momento de enviar información privada, mayor comodidad y accesibilidad al momento de trabajar desde un lugar fuera del campus.

Viabilidad

Esta investigación en factible por que se cuentan con personas calificados para realizar las configuraciones y programación necesarias para realizar la conexión al servidor VPN que se instalara, así como de las tecnologías correspondientes para establecer comunicación entre los deferentes campus de la Universidad Linda Vista.

Delimitaciones

La configuración para la comunicación entre los diversos campus de la Universidad Linda Vista.ubicada en pueblo nuevo solistahuacan correspondiente a la region norte del estado de chiapas, Mexico.

Definición de Términos

1. Autenticación - establecer la identidad de un usuario para transacciones seguras de e-commerce y VPN.

2. DES (Estándar de Encripción de Información, 3DES, Data Encryption Standard) - Un método de criptografía estándar del NIST de clave secreta que usa un llave de 56 bits (DES) o una llave de 168 bits (3DES).

3. Rechazo de Servicio (denominado DoS, por sus siglas en inglés Denial of Service) - un ataque de hacker diseñado para deshabilitar un servidor o red al saturarlo con solicitudes de servicio el cual previene a usuarios legítimos de accesar a los recursos de la red.

4. Encripción - el proceso de tomar toda la información que una computadora está enviando a otra y codificarla de una manera que sólo la otra computadora será capaz de decodificarla.

5. Firewall - a dispositivo de seguridad que controla el acceso desde Internet a una red local usando información asociada con paquetes TCP/IP para hacer decisiones sobre si se permiten o niegan accesos. Asociación Internacional de Seguridad Computacional (denominada ICSA, por sus siglas en inglés

6. Protocolo de Seguridad de Internet (IPSec, Internet Protocol Security) - un estándar IETF robusto de VPN que abarca autentificación y encripción de tráfico de datos sobre Internet.

7. Traductor de dirección de red (denominada NAT, por sus siglas en inglés Network Address Translation) - un estándar de seguridad que convierte múltiples direcciones IP en la red local privada a una dirección pública que es enviada al Internet.

8. Protocolo de Túnel Punto a Punto (denominado PPTP, por sus siglas en inglés Point-to-Point Tunneling Protocol) - un protocolo que esta integrado en el siste-

ma operativo Windows de Microsoft que permite acceso remoto con seguridad a redes corporativas sobre Internet (VPNs).

9. Inspección de Estado de Paquetes (Stateful Packet Inspection) - un dispositivo de seguridad ("firewall"), basado en la tecnología avanzada de filtrado de paquetes, que es transparente para los usuarios de la red local, no requiere configuración del cliente y asegura el arreglo más amplio de protocolos IP.

10. Túnel - la ruta a través de la cual un paquete de datos VPN con seguridad, viaja a través de la red interna.

11. Virus - programas de software dañino que atacan aplicaciones y archivos en memoria o discos.

12. VPN - Virtual Private Network

CAPÍTULO II

MARCO TEÓRICO

En la actualidad cada vez es mas necesario para las empresas contar con oficinas a una distancia considerable de la matriz, esto nos hace pensar en una forma de enlazar las distintas oficinas de la oficina central. la conectividad la podemos obtener de distintas formas con distintos proveedores con sus correspondientes variables en los costos, y a veces mucha inseguridad.

Redes Privadas Virtuales

Podemos definir a una red privada virtual como una unión de redes que permite extender una red local a través de una red pública de manera que exista comunicación como si estuvieran conectados a la misma red local.

Debido a que una red virtual privada trabaja en una red pública, el tema mas importante sería la seguridad de la información que compartimos ya que puede ser vista por cualquiera si no se toman las medidas necesarias. En una red pública como Internet existen varias personas que siempre están a la espera de capturar información valiosa, debido a eso una red privada virtual debe tener mecanismos de auntenticacion y de encriptacion que permitan al usuario un nivel de seguridad al enviar paquetes por Internet.

Componentes Básicos de Una VPN

El cifrado y las medidas de seguridad son la base de las Redes privadas virtuales. En cierto modo las VPN están sustituyendo a las WAN, a pesar de que estas se pueden operar mas fácilmente y tienen un bajo costo, pero no ofrecen seguridad apropiada para las empresas. los componentes que forman parte de una VPN son: (Shinder, 2013)

Servidor VPN. Es la Computadora que acepta conexiones VPN de clientes VPN. Encargado de administrar todos los clientes VPN y proporcionar la seguridad de la red.

Cliente VPN. Computadora que inicia una conexión VPN con un servidor VPN.

Túnel. Es la Porción de la conexión en la que los datos son encapsulados. Es la Conexión VPN.- Porción de la conexión en la cual los datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma porción de la conexión. Nota: Es posible crear un túnel y enviar los datos a través del túnel sin encriptación. Esta no es una conexión VPN porque los datos privados viajan a través de la red pública o compartida en una forma no encriptada y fácilmente visible e insegura.

Protocolos de túnel. Se utilizan para administrar los túneles y encapsular los datos privados. Existen varios protocolos de túnel que se estudiarán más adelante.

Datos del túnel. Datos que son generalmente enviados a través de un enlace punto a punto.

Red de tránsito. Red pública o compartida que permite el tránsito de los datos encapsulados. La red de tránsito puede ser Internet o una intranet privada. para simular un vínculo punto a punto en una VPN, los datos se empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta su destino. Para simular un vínculo privado los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexion en la que se encapsula y cifran los datos privados se denomina conexión VPN.

Internet Como Medio para VPN

En la actualidad el VPN se usa mucho en las empresas gracias al bajo costo en las operaciones. por ejemplo si una llamada de larga distancia costara 1.00 al dia tendria un costo de 60.00 si se trabajan 20 días al mes tendríamos un gasto de 1200.00 por persona, pero si comparamos con los 500.00 que algunos ISP proveen por acceso a Internet ilimitado, se ve claramente un ahorro considerable al usar una VPN. (CISCO, 2013a) | (Caldas, 2007)

Arquitectura de Una VPN

Existen dos tipos básicos de arquitecturas de VPN los cuales son:

1. VPN de acceso remoto

2. VPN de sitio a sitio

las VPN de acceso remoto se subdividen en VPN Dial-Up y VPN directa, a su vez las VPN de sitio a sitio o también llamadas VPN LAN a LAN o VPN POP a POP, estas se subdividen en VPN extranet y VPN intranet.

VPN de acceso remoto. Este tipo de VPN proporcionan acceso remoto a intranet o extranet empresarial. una VPN de acceso remoto ahorran dinero dinero a las empresas ya que en lugar de realizar llamadas de larga distancia, solo con establecer una conexión con el ISP local. el usuario solo debe hacer una conexión al servidor ISP de la compañía, a través de Internet, una vez que el usuario hizo conexión, podrá hacer uso de los recursos de la intranet privada de la empresa.

VPN Dial-Up. En este tipo de VPN el usuario realiza una llamada local a ISP utilizando el modem, aunque se trata de una conexión mas lenta es también la mas común, este tipo de VPN se usa mas entre los usuarios moviles, ya que no se puede tener una conexión de alta velocidad a todos los lugares a los que viaja.

VPN Directa. Este tipo de VPN se utilizan la tecnologías de conexión a Internet de alta velocidad, como DSL y modem de cable las cuales ya ofreces muchos ISP. se ocupa principal mente entre los tele trabajadores, también se emplea para obtener conexiones desde el hogar.

VPN de sitio a sitio. Esta alternativa a Frame Relay o a las redes WAN de línea alquilada permite a las empresas llevar los recursos de la red a las sucursales, las oficinas instaladas en casa y los sitios de partners comerciales. (CISCO, 2013b)

VPN Intranet. Una VPN de intranet se utiliza para la comunicacion interna de una compañia, enlazan la oficina central con todas las sucursales, ser rigen por las mismas normas como en cualquier red privada. Un enrutador realiza la conexion VPN de sitio a sitio que conecta dos partes de una red privada. el servidor VPN proporciona una conexion enrutada a la red que esta conectado el servidor VPN. (Shinder, 2004)

VPN Extranet. La característica de VPN Extranet es que permite a los proveedores de servicios de distribución del contenido de multidifusión IP se originé a partir de un sitio de la empresa a otros sitios de la empresa. Esta característica permite a los proveedores de servicios puedan ofrecer la próxima generación de servicios de extranet flexibles, lo que ayuda para que las asociaciones empresariales entre los diferentes clientes de la empresa VPN. (CISCO, 2006)

Requerimientos de Una Red Privada Virtual.

Para garantizar que una red privada virtual sea segura, este disponible y sea fácil de mantener es necesario cumplir con ciertos requisitos esenciales que una empresa debe tomar en cuenta antes de implementar una Red Privada Virtual (Brown, 2001)

Dichos requerimientos se enlistan abajo:

1. Disponibilidad
2. Control
3. Compatibilidad

4. Seguridad
5. Interoperabilidad
6. Confiabilidad
7. Autenticación de datos y usuarios
8. Sobrecarga de tráfico
9. Mantenimiento
10. Sin repudio

Disponibilidad. La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. No basta que el usuario tenga autorización para acceder a los servidores corporativos, si no puede conectarse debido a problemas de la red, por tanto se debe asegurar la disponibilidad en la parte física de la red.

Control. El control debe ser implementado por el supervisor o administrador de la Red Privada Virtual, sea este interno o externo dependiendo de la como se realizó la implementación de VPN. Debemos tomar en cuenta que por muy grande que sea la organización es posible tener una solo VPN, lo que facilitará al administrador de la VPN el control sobre la misma.

Compatibilidad. Debido que al utilizar tecnologías de VPN y de internet estas se basan en protocolo IP, por lo que la arquitectura interna del protocolo de red de la compañía debe ser compatible con el protocolo IP.

Seguridad. Hablar de seguridad y de red privada virtual, hasta cierto punto se podría decir que son sinónimos. La seguridad en una VPN abarca todo, desde el proceso de cifrado que se implementa hasta los servicios de autenticación de usuarios. Es necesario que se tenga muy en cuenta este término de seguridad, ya que se puede afirmar que una VPN sin seguridad no es una VPN.

Interoperabilidad. La interoperabilidad de una red privada virtual, es muy importante para la transparencia en la conexión entre las partes involucradas. Confiabilidad.- La confiabilidad es uno de los requisitos importantes que debe poseer en una Red Privada Virtual, pero esta confiabilidad se ve afectada en gran porcentaje en la VPN de Acceso Remoto en las que se sujeta a la confiabilidad que se tiene por parte del ISP, ya que si el servicio del ISP se interrumpe la conexión también y nosotros no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.

Autenticación de Datos y Usuarios. La autenticación de datos y de usuarios es sumamente importante dentro de cualquier configuración de Red privada Virtual. La autenticación de datos afirma que los datos han sido entregados a su destinatario totalmente sin alteraciones de ninguna manera. La autenticación de usuarios es el proceso en el que se controla que solos los usuarios admitidos tengan acceso a la red y no sufrir ataques por usuarios externos y maliciosos.

Sobrecarga de tráfico. La sobrecarga de tráfico es un problema de cualquier tipo de tecnología de redes, y por ende también es un problema inevitable, especialmente si tenemos una red privada virtual a través de un ISP. Tomando en cuenta que un

paquete enviado en una VPN es encriptado y encapsulado lo que aumenta de manera significativa la sobrecarga de tráfico en la red.

Mantenimiento. El mantenimiento, aspecto del que no se puede olvidar. Si la red privada virtual es implementada con los propios recursos de la empresa es necesario considerar que el mantenimiento debe estar soportado por el propio personal del departamento de sistemas, el cual debe estar capacitado para este fin. De no poseer el personal capacitado es preferible contratar servicio externos que se encarguen de la implementación y mantenimiento de la red privada virtual de la empresa.

Sin repudio. Consiste en el proceso de identificar correctamente al emisor, con la finalidad de tener claro desde donde proviene la solicitud. Si se considera que una VPN va a servir para contactar con los clientes, es necesario que este bien identificado de dónde proviene el pedido. Para poder realizar cualquier transacción comercial (comercio electrónico) por internet es necesario que esta transacción sea un proceso sin repudio. Nos podemos dar cuenta que nuevamente se está hablando de seguridad, una de las características fundamentales en una VPN. (Ramírez, 2013)

Ventajas de las Redes Privadas Virtuales.

El simple hecho de hablar de redes privadas virtuales, como se indicó anteriormente, viene a la mente el término de seguridad, así como también el bajo costo que esta tecnología necesita para implementarla y además su facilidad de uso, (Krause, 2013) En resumen, se puede decir que la implementación de una red privada virtual nos hace pensar en tres aspectos fundamentales y beneficiosos para nuestra empresa que son:

Ahorro en costos. El ahorro en costos de las redes privadas virtuales está asociado con diferentes factores que influyen en el paso de una tecnología anterior a una tecnología de redes privadas virtuales. La eliminación de líneas rentadas, al igual que las líneas por marcación son dos factores fundamentales que permitirán el ahorro en la implementación de una VPN, tomando en cuenta que al eliminar este tipo de comunicación también se elimina los costos de los demás dispositivos involucrados como puede ser equipos pbx, equipos de acceso remoto. También se eliminarán costos de instalación y configuración de dichos equipos de acceso remoto, entre otros costos.

Beneficios para el usuario final. El usuario final se ve muy beneficiado, ya sea un usuario que pertenezca a la propia empresa o un cliente. En la actualidad las empresas deben llegar al cliente, sin importar donde se encuentre éste, es por eso que se hace necesario que el cliente tenga acceso a los servicios y ya no se lo haga con comunicaciones telefónicas de larga distancia que son muy costosas, sino a través de un ISP local con un enlace más eficiente y menos costoso y además un enlace que va a estar disponible las 24 horas del día los 365 días del año. El mismo beneficio tendrán los usuarios remotos, facilitándoles el acceso a la información de la empresa en el momento que lo deseen, independiente del lugar en el que se encuentren.

Desventajas de las Redes Privadas Virtuales

Fiabilidad. Internet no es 100 porciento fiable, y fallos en la red pueden dejar incomunicados recurso de nuestra VPN.

Confianza entre sedes. Si la seguridad de un nodo o subred involucrada en la VPN se viese comprometida, eso afectaría a la seguridad de todas los componente de la VPN.

Interoperabilidad. Dado a las distintas soluciones disponibles para implementar una VPN, nos podemos encontrar incompatibilidades entre las usadas en los distintos nodos de la VPN. (Pena, 2013)

Topologias VPN

Asi como existen diferntes manera de adquirir e implementar una arquitectura de VPN, tambien existen muchas formas de colocar esta arquitectura en una topologia de VPN. La topologia nos indica el lugar que le corresponde a cada dispositivo en la configuracion de la red privada virtual.

Topologia de Cortafuegos. Este tipo de topología es la más común y posiblemente la más fácil de configurar para los que tienen un cortafuego colocado y solo desean la funcionalidad de la VPN. La configuración típica de cliente/VPN se trata de un usuario con un equipo portátil conectado a un servidor de la compañía, y en ella hay dos componentes que deben habilitarse para establecer la comunicación:

1. El dispositivo de cortafuego/VPN debe ejecutar algún tipo de código VPN.

2. La mayoría de los fabricantes de cortafuegos más conocidos que utilizan UNIX o Windows soportarán algún tipo de software cifrado.

3. El equipo portátil tiene una pila de VPN instalada. La pila de VPN se encuentra

entre los niveles 2 (enlace de datos) y 3 (red) del modelo OSI. (Víctor Hugo Taborda, 2004)

LAN a LAN. Este tipo de topología es la segunda más comúnmente utilizada. Esta topología también se utiliza entre oficinas y distintos clientes, creando un túnel VPN entre ambos. Si se utiliza tanto un cortafuego basado en NT como uno basado en UNIX, ambos utilizarán cifrado DES y serán capaces de comunicarse entre sí.

Cortafuego a intranet/extranet. Las intranets y extranets son los servicios de Internet más comunes hoy en día. En la tecnología VPN estos servicios tienen ahora un nivel adicional de cifrado. Normalmente, las intranets se utilizaban internamente por los empleados, y las extranets se utilizaban externamente por los clientes. Ahora, con la tecnología VPN, se puede tener acceso internamente o externamente a cualquier servicio. Esto tiene dos condiciones: primero, se cuenta con flexibilidad para que una máquina se encargue de ambos servicios y por lo tanto se reduce la redundancia; la segunda condición es la seguridad, ahora existe una forma para que los usuarios externos tengan accesos a estos servidores.

Tramas O ATM. Las VPN pueden configurarse sobre una infraestructura compartida tal como ATM o topologías de redes basadas en tramas. Los negocios que ejecutan sus propias intranets sobre esta topología de VPN tienen la misma seguridad, facilidad de administración y confiabilidad que en sus propias redes privadas. Este tipo de topología generalmente se configura de dos maneras. La primera es IP sobre una infraestructura de red de tramas/ATM. Esta combinación combina el nivel

de aplicación de los servicios IP sobre la capacidad de una red ATM. Dependiendo de la configuración del equipo, los paquetes IP se convierten en celdas y se transfieren sobre una red ATM. El proceso de cifrado se ejecuta en estos paquetes antes de la conversión a celdas, y las celdas que contienen la carga IP cifrada se conmutan al destino final. La segunda opción es la del grupo de trabajo de Conmutación de etiquetas multiprotocolo (MPLS) del Grupo de trabajo de ingeniería de Internet (IETF). En esta topología de red, los conmutadores inteligentes reenvían dinámicamente el tráfico IP en paralelo junto con el tráfico ATM en la misma red ATM. Al paquete se le aplica un campo que contiene un identificador único, que identifica el destino final. Los conmutadores de esta red ATM examinan este campo y lo reenvían a su destino apropiado. El atributo de seguridad de esto es que el paquete sólo se reenvía a su destino, evitando así el espionaje. Cualquier proceso de cifrado que puede utilizarse aquí sólo se aplica a la porción de datos, antes de enviarlo a la nube ATM.

VPN de hardware . Se trata de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen equipadas con software que se ejecuta en el cliente, para ayudar a administrar el dispositivo, y otras se las puede administrar mediante el explorador de Internet. Por ser un dispositivo de hardware se cree que las VPN instaladas con estos equipos son mucho más rápidas que los tipos basados en software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado mucho más rápido. Aunque esto puede ser verdad, no todos ofrecen una característica de administración centralizada (Brown, 2001)

VPN/NAT. Aunque la Traducción de Direcciones de Red (NAT) no es una VPN, se debe discutirla ya que muchas organizaciones lo tienen implementado, y los dispositivos VPN se ven afectados directamente por los procesos de NAT. La traducción de direcciones de red es el proceso de cambiar una dirección IP (por lo general la dirección privada de una organización) a una dirección IP pública enrutable. NAT proporciona un mecanismo para ocultar la estructura de la dirección privada de una organización. Utilizar la traducción de direcciones de red no es complicado, pero la ubicación del dispositivo VPN es importante (Brown, 2001). Si implementa a NAT en un paquete de VPN, ese paquete puede ser descartado; se debe recordar que una VPN es una configuración de IP a IP. La figura 5.8 muestra el flujo de tráfico que tiene lugar en un cortafuego que implementa a NAT mientras que el dispositivo VPN se encarga de la autenticación de usuarios.

Estas dos reglas deben seguirse cuando se utilice NAT y VPN:

1. Para paquetes de salida. Si tienen que pasar por NAT y ser parte de una VPN, NAT debe aplicarse antes de que el dispositivo VPN cifre los paquetes.

2. Para tráfico de VPN entrante. NAT debe aplicarse después de que el cifrado de VPN se haya eliminado del paquete.

Túneles de VPN anidados.. Los túneles de VPN anidados pueden considerarse como un túnel dentro de otro túnel. Existen muchas formas para hacer túneles anidados, una forma de emplearlos es cuando una organización requiere implantar seguridad punto a punto (Brown, 2001).

1. El cliente PPTP realiza el proceso de cifrado en los datos desde la aplicación.

2. Después, reenvía el flujo de datos cifrados al dispositivo de cortafuego/VPN, el cual añade cifrado DES al paquete. El cifrado DES puede implementarse como parte d la norma IPSec.

3. El paquete es recibido por el dispositivo remoto de la VPN, el cual revisa la autenticación, quita el cifrado DES y lo envía a su destino final, que es el servidor PPTP.

4. El servidor PPTP descifra el paquete PPTP y lo reenvía a las aplicaciones de nivel superior. Antes de que dos dispositivos de cortafuego/VPN puedan realizar cualquier proceso de cifrado / descifrado, primero deben estar configurado entre ellos. Comúnmente se recomienda utilizar IPSec y PPTP en combinación.

Balance de carga y sincronizacíon. La tecnología VPN puede tener balance de carga. El balance de carga es el proceso de distribuir las necesidades de procesamiento de las VPN entre varios servidores. La sincronización es el proceso de sincronizar dispositivos VPN. La configuración de un brazo (en paralelo), es una topología típica cuando se utiliza el balance de carga y la sincronización. Gracias a esto las VPN pueden crecer.

Topología de conmutacíon de VPN. Existen productos en el mercado llamados conmutadores de VPN. Son conmutadores de nivel 3 que crean túneles bajo solicitud. Tienen la capacidad para crear y asignar características de túneles y conmutar tráfi-

co multiprotocolo. Supuestamente realizan cifrado, encapsulamiento y enrutamiento multiprotocolo a velocidad de cable. Además, tienen una característica útil para soportar una conmutación basada en las políticas del protocolo de red. Estos conmutadores de VPN incluyen software para mantenimiento remoto que proporciona capacidad de planeación, tolerancia frente a las fallas e información estadística, como la utilización de túneles y la calidad del servicio de supervisión. Los túneles se configuran a través de una consola de administración y se crean y conmutan bajo solicitud a los destinos respectivos. Aunque generalmente son fáciles de configurar y de mantener, no son cortafuegos. Por lo tanto, no ofrecen la protección que podría ofrecer un cortafuego. (Schmidt, 2001)

VoIP

La tecnología de voz sobre el Internet o VoIP por el acrónimo de *Voice over Internet Protocol*, es una forma nueva de hacer y recibir llamadas telefónicas utilizando una conexión de Internet de banda ancha (broadband) en lugar de una línea telefónica corriente.

Qué Es la Telefonía IP?

La telefonía IP permite comunicaciones de voz sobre redes basadas en protocolo Internet (IP). Unifica las múltiples delegaciones que una organización pueda tener (incluidos trabajadores móviles) en una única red convergente. Además promete ahorro de costes al combinar la voz y los datos en una misma red que puede ser

mantenida centralizadamente, así como ahorrar las elevadas tarifas repercutidas por llamadas entre delegaciones.

Conceptos Generales de VoIP

Desde el punto de vista técnico, la red telefónica tradicional (PSTN) no ha tenido una gran evolución desde su invención a fines del siglo XIX. A la vez, existe una tendencia cada vez mayor a enviar la señal de voz en forma digital, en paquetes a través de la red de datos, en lugar de utilizar la red telefónica convencional (PSTN). Esto muestra que la convergencia de la voz y los datos hacia una misma red, es y será una realidad del siglo XXI. El grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP, es llamado Voz sobre IP (VoIP). Es una tecnología con un crecimiento muy alto, en la cual apostaron muchas empresas. La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) usuales de la red PSTN. La reducción en los costos se debe principalmente a la utilización de una misma red para transportar voz y datos; en especial cuando los usuarios no utilizan la totalidad de la capacidad de su red, la cual puede ser usada para VoIP sin un gran costo adicional. Otro beneficio a destacar, es la amplia gama de soluciones comerciales, que permiten construir redes de telefonía con servicios adicionales, tales como buzón de voz, Voice-mail, multiconferencia, servidor vocal interactivo (IVR), distribución automática de llamadas, entre otras. Al mismo tiempo, se crearon comunidades de programadores con el fin de desarrollar soluciones Open Source de VoIP. Los programas Open Source tuvieron un gran éxito en los ámbitos empresariales y universitarios debido a su eficiencia, lo que los volvió

competitivos, en muchas áreas, en relación a las soluciones propietarias existentes. Dichos programas Open Source buscaron evitar los problemas inherentes a los sistemas propietarios tradicionales con lo que lograron; minimizar los costos, mejorar la flexibilidad, el mantenimiento y soporte de equipos, así como también permitir que cada usuario pueda tener el control de su propio sistema. El desarrollo de aplicaciones open source, hace posible el fácil acceso y en forma económica, a sistemas de comunicación VoIP y a información asociada (manuales, tutoriales, HowTo, URL oficiales, foros, etc) lo que facilita la implementación de estos sistemas.

Es posible tener acceso a una central telefónica PBX (Asterisk), a la cual se le conecten usuarios VoIP mediante softphones ambos disponibles en Open Source. Con esto se puede realizar una implementación donde se les asigna extensiones telefónicas y buzones de voz a estos usuarios, con lo cual se pueden comunicar entre sí o dejarse mensajes de voz en caso que el destinatario no esté disponible. Además es posible agregar una funcionalidad más avanzada que permita que el mensaje de voz sea enviado al correo electrónico de su destinatario con un cierto formato. Para ello se requiere el uso de un servidor de correo, también disponible en Open Source.

Arquitectura de red para VoIP. El propio Estándar define tres elementos fundamentales en su estructura:

1. Terminales: son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

2. Gatekeepers: son el centro de toda la organización VoIP, y son el sustituto pa-

ra las actuales centrales. Normalmente implementan por software, en caso de existir, todas las comunicaciones que pasen por él.

3. Gateways: se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario. Con estos tres elementos, la estructura de la red VoIP podría ser la conexión de dos delegaciones de una misma empresa. La ventaja es inmediata: todas las comunicaciones entre las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva.

4. Protocolos de VoIP: son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación. o Por orden de antigüedad (de más antiguo a más nuevo):

5. H.323 - Protocolo definido por la ITU-T;

6. SIP - Protocolo definido por la IETF;

7. Megaco (También conocido como H.248) y MGCP - Protocolos de control;

8. UNIStim - Protocolo propiedad de Nortel(Avaya);

9. Skinny Client Control Protocol - Protocolo propiedad de Cisco;

10. MiNet - Protocolo propiedad de Mitel;

11. CorNet-IP - Protocolo propiedad de Siemens;

12. IAX - Protocolo original para la comunicación entre PBXs Asterisk (Es un estándar para los demás sistemas de comunicaciones de datos,[cita requerida] actualmente está en su versión 2, IAX2);

13. Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype;

14. IAX2 - Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX;

15. Jingle - Protocolo abierto utilizado en tecnología XMPP;

16. MGCP- Protocolo propietario de Cisco;

17. weSIP- Protocolo licencia gratuita de VozTelecom.

Como hemos visto VoIP presenta una gran cantidad de ventajas, tanto para las empresas como para los usuarios comunes. La pregunta sería ¿por qué no se ha implantado aún esta tecnología?. A continuación analizaremos los aparentes motivos, por los que VoIP aún no se ha impuesto a las telefonías convencionales.

Parámetros de la VoIP. Este es el principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP. Garantizar la calidad de servicio sobre Internet, que solo soporta "mejor esfuerzo"(best effort) y puede tener limitaciones de ancho de banda en la ruta, actualmente no es posible; por eso, se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

Códecs. La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de códecs que garanticen la codificación y compresión del audio o

del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda utilizada suele ser directamente proporcional a la calidad de los datos transmitidos. Entre los codecs más utilizados en VoIP están G.711, G.723.1 y el G.729 (especificados por la ITU-T). Estos Codecs tienen los siguientes anchos de banda de codificación:

1. G.711: bit-rate de 56 o 64 Kbps.
2. G.722: bit-rate de 48, 56 o 64 Kbps.
3. G.723: bit-rate de 5,3 o 6,4 Kbps.
4. G.728: bit-rate de 16 Kbps.
5. G.729: bit-rate de 8 o 13 Kbps.

Esto no quiere decir que es el ancho de banda utilizado, ya que hay que sumar el tráfico de por ejemplo el Codec G729 utiliza 31.5 Kbps de ancho de banda en su transmisión.

Retardo o latencia. Una vez establecidos los retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms, que viene a ser 1,5 décimas de segundo y ya produciría retardos importantes.

Calidad del servicio. Para mejorar el nivel de servicio, se ha apuntado a disminuir los anchos de banda utilizados, para ello se ha trabajado bajo las siguientes iniciativas:

1. La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.

2. Compresión de cabeceras aplicando los estándares RTP/RTCP. Para la medición de la calidad de servicio QoS, existen cuatro parámetros como el ancho de banda, retraso temporal (delay), variación de retraso (jitter) y pérdida de paquetes. Para solucionar este tipo de inconvenientes, en una red se puede implementar tres tipos básicos de QoS:

3. Best effort: (en inglés, mejor esfuerzo) Este método simplemente envía paquetes a medida que los va recibiendo, sin aplicar ninguna tarea específica real. Es decir, no tiene ninguna prioridad para ningún servicio, solo trata de enviar los paquetes de la mejor manera.

4. Servicios Integrados: Este sistema tiene como principal función pre-acordar un camino para los datos que necesitan prioridad, además esta arquitectura no es escalable, debido a la cantidad de recursos que necesita para estar reservando los anchos de banda de cada aplicación. RSVP (Resource Reservation Protocol) fue desarrollado como el mecanismo para programar y reservar el ancho de banda requerido para cada una de las aplicaciones que son transportados por la red.

5. Servicios Diferenciados: Este sistema permite que cada dispositivo de red tenga la posibilidad de manejar los paquetes individualmente, además cada router y

switch puede configurar sus propias políticas de QoS, para tomar sus propias decisiones acerca de la entrega de los paquetes. Los servicios diferenciados utilizan 6 bits en la cabecera IP (DSCP Differentiated Services Code Point). Los servicios para cada DSCP son los siguientes:

6. La priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:

7. PQ (Priority Queueing): Este mecanismo de priorización se caracteriza por definir 4 colas con prioridad Alta, media, normal y baja, Además, es necesario determinar cuales son los paquetes que van a estar en cada una de dichas colas, sin embargo, si estas no son configuradas, serán asignadas por defecto a la prioridad normal. Por otra parte, mientras que existan paquetes en la cola alta, no se atenderá ningún paquete con prioridad media hasta que la cola alta se encuentre vacía, así para los demás tipos de cola.

8. WFQ (Weighted fair queuing): Este método divide el tráfico en flujos, proporciona una cantidad de ancho de banda justo a los flujos activos en la red, los flujos que son con poco volumen de tráfico serán enviados más rápido. Es decir, WFQ prioriza aquellas aplicaciones de menor volumen, estas son asociadas como más sensibles al delay (retardo) como VoIP. Por otra parte, penaliza aquellas que no asocia como aplicaciones en tiempo real como FTP.

9. CQ (Custom Queueing): Este mecanismo asigna un porcentaje de ancho de ban-

da disponible para cada tipo de tráfico (voz, video y/o datos), además especifica el numero de paquetes por cola. Las colas son atendidas según Round Robin (RR). El método RR asigna el ancho de banda a cada uno de los diferentes tipos de tráfico existentes en la red. Con este método no es posible priorizar tráfico ya que todas las colas son tratadas de igual manera.

10. La implantación de IPv6, que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

Ventajas. La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada (PSTN). Algunos ahorros en el costo son debidos a utilizar una misma red para llevar voz y datos, especialmente cuando los usuarios tienen sin utilizar toda la capacidad de una red ya existente la cual pueden usar para VoIP sin coste adicional. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis en contraste con las llamadas de VoIP a PSTN que generalmente cuestan al usuario de VoIP. El desarrollo de codecs para VoIP (aLaw, G.729, G.723, etc.) ha permitido que la voz se codifique en paquetes de datos cada vez más pequeños. Esto deriva en que las comunicaciones de voz sobre IP requieran anchos de banda muy reducidos. Junto con el avance permanente de las conexiones ADSL en el mercado residencial, éste tipo de comunicaciones están siendo muy populares para llamadas internacionales. Hay dos tipos de servicio de PSTN a VoIP: "Discado Entrante Directo"(Direct Inward Dialling: DID) y "Números de acceso". DID

conecta a quien hace la llamada directamente con el usuario VoIP, mientras que los Números de acceso requieren que este introduzca el número de extensión del usuario de VoIP. Los Números de acceso son usualmente cobrados como una llamada local para quien hizo la llamada desde la PSTN y gratis para el usuario de VoIP. Estos precios pueden llegar a ser hasta 100 veces más económicos que los precios de un operador locales.

Desventajas.

1. Calidad de la llamada. Es un poco inferior a la telefónica, ya que los datos viajan en forma de paquetes, es por eso que se pueden tener algunas perdidas de información y demora en la transmisión. El problema en si de la VoIP no es el protocolo sino la red IP, ya que esta no fue pensada para dar algún tipo de garantías. Otra desventaja es la latencia, ya que cuando el usuario está hablando y otro usuario está escuchando, no es adecuado tener 200ms (milisegundos) de pausa en la transmisión. Cuando se va a utilizar VoIP, se debe controlar el uso de la red para garantizar una transmisión de calidad.

2. Robos de Datos. Un cracker puede tener acceso al servidor de VoIP y a los datos de voz almacenados y al propio servicio telefónico para escuchar conversaciones o hacer llamadas gratuitas a cargo de los usuarios.

3. Virus en el sistema. En el caso en que un virus infecta algún equipo de un servidor VoIP, el servicio telefónico puede quedar interrumpido. También pueden verse afectados otros equipos que estén conectados al sistema. Suplantaciones de

ID y engaños especializados. Si uno no está bien protegido pueden sufrir fraudes por medio de suplantación de identidad.

Asterisk. Asterisk es un software Open Source que proporciona funcionalidades de central telefónica (PBX). Originalmente fue creado para sistemas Linux, actualmente existen versiones para sistemas OpenBSD, FreeBSD, Mac OS X, Solaris y Windows. Igualmente Linux sigue siendo la que más soporte presenta. Permite la conexión de teléfonos analógicos (para los cuales es necesario utilizar tarjetas electrónicas telefónicas FXO o FXS), teléfonos digitales, terminales IP y softphones ya que soporta muchos protocolos de VoIP como ser SIP, IAX, H.323 y MGCP Cuenta con servicios de buzón de voz, creación de extensiones, mailserver, envío de mensajes de voz a e-mail, llamadas en conferencia, IVR, distribución automática de llamadas, entre otras. A su vez, cada usuario puede crear su propias funcionalidades a través de la creación de un dialplan o añadiendo módulos en lenguajes de programación soportados por Linux.

Dialplan. Es el corazón del sistema Asterisk, en él se define como se van a manejar las llamadas. Consiste en un conjunto de instrucciones o pasos que Asterisk debe seguir y es completamente customizable. El dialplan se configura en el archivo extensión.conf. Dentro de él se manejan los siguientes conceptos: contextos, extensiones, prioridad y aplicaciones.

Contextos. Los dialplan están separados en secciones llamadas contextos. El contexto es uno de los parámetros que se especifica al definir un canal, por lo que

es el punto de partida para que el dialplan pueda realizar la conexión al mismo. Uno de los usos más importantes del contexto es la seguridad. Permite establecer una comunicación (por ejemplo de larga distancia) sin que quede disponible para otros usuarios. Las extensiones que se encuentran definidas dentro de un contexto, no puede interactuar (a no ser que se le permita) con una extensión de otro contexto. Se determina con su nombre entre [ ] y tiene una extensión máxima de 79 caracteres. Todas las instrucciones situadas debajo de su nombre, son parte del mismo (hasta el comienzo de uno nuevo).

Extensions. En el mundo de las comunicaciones, una extensión se refiere al número que identifica el ring de cierto teléfono. En Asterisk es mucho más que eso. La extensión es la que le indica a Asterisk que pasos debe seguir cuando esa extensión es requerida. La sintaxis de una extensión es la palabra exten seguida del signo de igual y el de mayor, como se muestra a continuación: exten => Esta expresión es seguida por el número de la extensión (el cual puede ser una combinación de números y letras), la prioridad (cada extensión esta compuesta por varios pasos, los cuales se ejecutan en el orden establecido por la prioridad), y por la aplicación (o comando) que es la que realiza la acción. Por lo cual una extensión tiene la siguiente sintaxis: exten => número, prioridad, aplicación()

Prioridad. La prioridad es un número que indica el orden en el que se ejecutan los pasos de la extensión. Generalmente se suele poner la prioridad 1 (en el primer paso a ejecutarse) y luego una n que significa “next”, la prioridad anterior +1. Esto es así para poder agregar pasos intermedios, en un plan de numeración ya existente, sin

tener que renumerar las prioridades manualmente, lo cual puede tornarse engorroso. A continuación se muestra un ejemplo: exten => 123,1,Answer() exten => 123,n,hacer algo exten => 123,n,hacer algo más exten => 123,n,Hangup() Se pueden colocar etiquetas a la prioridad de manera de poder referirse a ella no solo por su número. Para ello se coloca la etiqueta entre paréntesis curvos a continuación del número de prioridad. exten => 123,n(etiqueta),aplicación()

Aplicaciones. Las aplicaciones son aquellas que especifican una acción concreta en el canal, por ejemplo, reproducir un cierto sonido, aceptar un tono de entrada, terminar una llamada, etc. Hay algunas aplicaciones que no requieren de información adicional (argumentos) como ser Answer() y Handup(). Hay otras a las que se les debe o puede pasar argumentos. Estos se deben colocan entre paréntesis a continuación del nombre de la aplicación. Si son varios argumentos se separan con comas “,” .

Softphones. Un softphone es un software que provee funcionalidades de un teléfono convencional. Generalmente opera en un entorno Voz sobre IP. Está basado en un protocolo de señalización, el cual puede ser estandarizado (SIP, H.323, IAX) o privativo. Existen diversos softphones disponibles, algunos de estos son: sjphone, X-Lite, Ekiga, kphone y kiax.

FreepVox. FreePBX ofrece un interfaz GUI Html (interfaz gráfica de usuario) para administración de una centralita IP basada en Asterisk, muy fácil de usar pero con gran capacidad. También está basado en Open Source GPL. Permite configurar fácilmente un sistema Asterisk, cubriendo los requisitos tanto de pequeñas como de

grandes empresas. Puede mantener las bases de datos de usuarios y extensiones, así como todas las funciones de valor añadido. Por citar las más importantes:

1. Dialplan de llamadas entrantes y salientes.
2. IVR (Recepcionista digital interactiva) – Operadora automática.
3. Time conditions – Gestión de llamadas entrantes según horario y fecha.
4. Grupo de llamadas (Ring Groups): Round-Robin, todas a la vez, etc.
5. Follow-me.
6. ACD – Sistema de colas y agentes.
7. Monitorización de llamadas.
8. Sistema de mensajería vocal.
9. Música en espera.
10. Sala de Conferencias.
11. Grabación de las llamadas (sólo recomendado para pequeños volúmenes).

Sistema Operativo

Segun IT World (Tecnología Informática) varias situaciones harán que aumente el número de instalaciones de la edición de servidor de Ubuntu entre ellas:

La disponibilidad de Ubuntu Server al poder descargar los CDs. Amplia documentación disponible, la mayoría mantenida por la comunidad. El costo es mucho menor si lo comparas con soluciones de RedHat o Novell (otros desarrolladores de Linux). La preocupación que la gente tiene sobre el futuro incierto de Solaris, el sistema operativo antes, de Sun Microsystems, ahora propiedad de Oracle. El ciclo de actualizaciones de 6 meses y el soporte de las versiones LTS (Soporte Técnico Extendido) de hasta 5 años para la edición de servidor, son alternativas que no ofrecen otros proveedores, y con la llegada de Landscape Canonical (grupo encargado del desarrollo de Ubuntu) pone al alcance de cualquier empresa u organización la habilidad de administrar, actualizar (parches o updates) de manera centralizada tanto Servidores como Escritorios de Ubuntu, así como servicios de cloud computing utlizando EC2 de Amazon (servicio web que proporciona capacidad informática con tamaño modificable en la nube). Las opciones que la distribución provee para simplificar la instalación y configuración de servicios como Apache o Postfix en las que ahorran valioso tiempo del administrador. El soporte técnico que está disponible para solucionar cualquier problema que se presente, una enorme comunidad activa que provee documentos, foros, reportes de bugs que, sin mentir, difícilmente cualquier otra comunidad puede igualar. También existe una opción de soporte comercial por parte de Canonical con el que se puede enfrentar cualquier evento que se presente.

Cabe destacar que el hecho de contar con el soporte de Canonical, Ubuntu genera cierta garantía al momento de su elección entre servidores de Linux.

CAPÍTULO III

PROPUESTA

La presente memoria pretende diseñar una forma de conexión entre los campus de la Universidad Linda Vista, ahorrando en las comunicaciones, poniendo a disposición de los catedráticos y administrativos así como de alumnos que requieran de información valiosa en cualquier lugar que se encuentren, usando las Redes Privadas Virtuales, asi como tambien proveer de un a linea de comunicacion con internet como medio de transmicion,

Diseño

Se a montará un servidor de VPN PPTP en Ubuntu Server. De esta manera no tendremos que recurrir a usar servicios de terceros cuando necesitemos navegar de forma segura desde sitios públicos. tambien se configurara un servidor para VoIP con el software bajo licencia GPL Asterisk.

Requerimientos basicos:

1. PC con Ubuntu Server 12.04.3 LTS
2. Conexion a internet
3. Tener una dirección IP estática,

4. Tener el puerto PPTP (1723 TCP y 1723 UDP) abierto

Sistema Operativo

Ya que uno de los objetivos es ahorrar recursos económicos, el sistema operativo que se usará sera una distribución de linux: ubuntu server. ya que proporciona las características necesarias para el buen funcionamiento del servidor. se recurrira a la terminal viene por defecto en la distribucion de ubuntu server, ya que no cuenta con una interfaz grafica nativa, si se desea se puede incluir una interfaz grafica sin embaro para efectos de optimizar recursos no se utilizara ninguna interfaz.

Código

Para configurar un servidor VPN con el protocolo PPTP se tiene que configurar la pc con ip statica para ello se edita el siguiente script:

```
sudo nano /etc/network/interfaces
```

se comenta la linea "iface eth0 inet dhcp" y escribimos abajo

```
iface eth0 inet static
address (direccion de la maquina)
netmask (Mascara de subred)
gateway (puerta de enlace predeterminado)
dns-nameservers (los dns de preferencia del ISP)
```

se guarda y se reinicia la interface de red con

```
/etc/init.d/networking restart
```

Instalación de Paquetes

En el terminal tecleamos la siguiente orden:

```
sudo apt-get install pptpd
```

apt-get detecta que para que se pueda instalar el paquete pptpd necesita, además, el paquete bcrelay. Antes de realizar acción alguna pide nuestra aprobación. Dado que estamos de acuerdo presionamos la tecla "S" y luego ENTER para que comience la descarga y posterior instalación de los paquetes.

Configuración

Una vez finalizado el proceso se iniciará el servidor PPTP automáticamente, pero aún no está configurado, para lo cual ejecutaremos:

```
sudo nano /etc/pptpd.conf
```

Tras ejecutarlo aparecerá en la misma terminal, el editor nano. Usando los cursores bajamos hasta el final del todo e insertamos, como si se tratara del bloc de notas, las líneas

```
localip 10.10.10.1
remoteip 10.10.10.100-200,10.10.10.245
```

Explicación:. Primera línea: Especificamos cuál será la dirección IP de nuestro servidor dentro de la VPN. Para que no haya conflicto con las direcciones IP "domésticas", hemos seleccionado un rango de direcciones distinto. Segunda línea: Especifica el rango de direcciones que usaremos para asignar a los clientes. En la parte anterior a la "," (coma) hemos especificado un rango y detrás una dirección simple. Con esto hemos querido mostraros las dos posibles formas de especificar las direcciones de los clientes, es decir, que pueden especificar simplemente un rango. Para guardar los cambios presionamos "Control + O" y para salir "Control + X".

Añadiendo Usuarios

Ahora vamos a añadir usuarios a nuestra VPN. Para hacerlo modificaremos el archivo chap-secrets: sudo nano /etc/ppp/chap-secrets como vemos en la imagen 1. Ahora guardamos y salimos, ya sabéis "Control + O" y "Control + X"

Configurando Iptables

Hasta este punto ya tenemos todo lo referente a nuestra VPN configurado, tan sólo queda configurar el cortafuegos de Ubuntu para que permita el acceso a las

conexiones entrantes y redirija el tráfico. Para que la configuración se mantenga con cada reinicio modificaremos el script rc.local: sudo nano rc.local

Vamos hasta el final del fichero e insertamos ANTES de la última línea lo siguiente:

```
iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
```

como vemos en la imagen 2.

Explicacion:. 10.10.10.0/24 : Rango de direcciones que elegimos cuando estábamos configurando PPTPD. eth0 : Nombre de la interfaz de red. En nuestro caso se trata de cable, si fuera WiFi recibiría el nombre de wlan0 . Una vez realizados los cambios, cerramos y guardamos como hasta ahora.

Ahora vamos a proceder a activar el IP forwarding, para ello vamos a modificar el archivo/etc/sysctl.conf: sudo nano /etc/sysctl.conf

Buscamos la línea:

```
#net.ipv4.ip_forward=1
```

```
#net.ipv4.ip_forward=1
net.ipv4.ip_forward=1
```

Guardamos los cambios y cerramos el archivo. podemos ver el ejemple en la figura 3.

Aunque en un principio podríamos aplicar los cambios sin necesidad de reiniciar el ordenador, creemos que es interesante verificar que después de reiniciar todo continúa funcionando perfectamente. Así que vamos a reiniciar el ordenador desde el propio terminal:

```
Sudo reboot
```

Tester del Servidor VPN

Para testear el servidor se iniciara una nueva conexion VPN para ello podemos ir a inicio y teclear VPN configurar una conexion de red privada virtual(VPN) pedira los datos del servidor ver imagen 4

El siguiente paso es introducir los datos de usuario. como vemos en la imagen **??**

muchas maquinas presentan el inconveniente al tratar entrar a internet, lo cual se puede arreglar de la siguiente forma:

editamos el script ip-up, para ello se edita con el siguiente comando:

```
Sudo nano /etc/ppp/ip-up
```

y al final se escribe la siguiente linea:

```
/sbin/ifconfig $1 mtu 1400
```

guardamos con “Control + O“ y para salir “Control + X“.
luego se edita el script pptpd-options con el siguiente codigo:

```
sudo nano /etc/ppp/pptpd-options
```

y en la linea

```
#ms-dns 10.0.0.1
#ms-dns 10.0.0.1
```

se quitan los comentarios y se agregan los dns del ISP guardamos con “Control + O“ y para salir “Control + X“. y se reinicia la maquina con:

```
Sudo reboot
```

Servidor VoIP

Como se menciona en el marco teorico el servicio de VoIP sera reaalizado con el sistema de asterisk que se encontrara instalado en el mismo servidor VPN. Las configuraciones necesarias para instalar dicho servidor se enumeran a continuacion:

Instalacion de Asterisk. Para poder instalar el servicio de ASTERISK debemos de hacerlo escribiendo en consola el siguiente comando:

```
sudo apt-get install asterisk
```

Esperamos que culmine la instalación y procedemos a configurar el servidor. NOTA: También está disponible una versión comprimida de ASTERISK en su página web, la cual se compila e instala, no la usamos porque a veces el servidor no funciona correctamente por la falta de dependencias, es decir la diferencia de instalar por consola y

por comprimido es que por consola instala todas las dependencias necesarias, lo cual no hace la versión comprimida.

Edición de los siguientes archivos. Archivo /etc/asterisk/manager.conf Escribimos en consola:

```
sudo nano /etc/asterisk/manager.conf
```

Debemos borrar todo lo escrito, y reemplazarlo por lo siguiente:

```
[general]
enabled = yes
webenabled = yes
port = 5038
[admin]
secret = asterisk
deny=0.0.0.0/0.0.0.0
permit=0.0.0.0/0.0.0.0
read = system,call,log,verbose,agent,user,config,dtmf,reporting,cdr,dialplan
write = system,call,agent,user,config,command,reporting,originate
```

Explicacion :

1. Habilitar el "manager"de asterisk
2. Habilitar el acceso via web al "manager"para gestionar nuestra PBX
3. Definir el port de acceso para el "manager"
4. Crear el usuario ”admin” con la password ”asterisk”
5. Permitir el acceso al manager desde cualquier IP
6. Setear los permisos del usuario .ªdmin"para lectura (read) y escritura (write)

guardamos con “Control + O“ y para salir “Control + X“.

el siguiente archivo es http.conf y se escribe el siguiente comando:

```
sudo nano /etc/asterisk/http.conf
```

Al final del archivo se agrega lo siguiente:

```
enabled=yes
bindaddr=0.0.0.0
bindport=8088
enablestatic=yes
redirect = / /static/config/index.html
```

quedaria como vemos en la imagen 7 guardamos con “Control + O“ y para salir “Control + X“.

Instalacion y configuración de FreepVx. Ahora vamos a instalar ASTERISK-GUI como administrador web. NOTA: La versión más reciente al momento de hacer este tutorial es: asterisk-gui-2.1.0- rc1.tar.gz . Entonces copiamos la ruta del archivo y ejecutamos en consola lo siguiente:

```
sudo wget http://downloads.asterisk.org/pub/telephony/asteriskgui/releases/asterisk-gu
sudo cp asterisk-gui-2.1.0-rc1.tar.gz /usr/src/
sudo tar xvfz asterisk-gui-2.1.0-rc1.tar.gz
sudo ln -s /usr/src/asterisk-gui-2.1.0-rc1 asterisk-gui
sudo cd asterisk-gui
sudo ./configure
sudo make
sudo make install
sudo make checkconfig
```

al final se reinicia el servicio de asterisk

```
Sudo service asterisk restart
```

NOTA: Cada vez que realicemos una modificación debemos de reiniciar el ASTERISK. Si instalamos el ASTERISK por comprimido no nos aparecerá el servicio.

Ahora abrimos el navegador y escribimos en la barra de direcciones lo siguiente:

```
http://[ip-servidor]:8088
```

Si no conocemos la IP de nuestro servidor efectuamos el siguiente comando en consola: ifconfig.

Escribimos el usuario y la contraseña configurada en el archivo /etc/asterisk/-manager.conf

Configuración de FreepVx en la interfaz GUI HTML. Se configuraran los planes, los usuarios y el buzón de voz. Se debe realizar el primer y segundo paso en ese

orden, ya que no se puede crear usuarios sin tener planes. podemos ver una captura de pantalla de la pagina principal de esta interfax en la imagen 8

A. Crear un plan Para crear un plan debemos hacer click en el menú izquierdo en la opción Dial Plans Y hacer click en NewDialPlan, nos abrirá una ventana que se muestra en la imagen 9

Se escribe el nombre del plan y se pone SAVE. Notar que habilitamos todas las opciones (incluida la de VOICEMAIL). NOTA: Se pueden agregar más planes de acuerdo al criterio.

B. Crear los usuarios Ahora se procedera a crear los usuarios, para ello se le da click en el menú izquierdo en Users .Luego en Create New User y se muestra la imagen 10 Explicacion de la configuracion: Extension: Es el numero SIP para el usuario, este valor no se puede modificar inicializa en (6000) y es auto numérico, es decir incrementa en 1 al agregar un nuevo usuario (6001, 6002, 6003,. . . .). CallerIdName: Es el nombre de usuario para la línea, puede ser texto o numero (Nombre de usuario). DialPlan: Seleccionamos el plan que ya configuramos anteriormente. CallerIdNumber: Un numero de referencia del usuario para identificarlo en la red. Enable VoiceMail for this User: Habilita la opción de buzon de voz para el usuario. VoiceMail Access PIN Code (opcional): Este es un código numérico para que el usuario pueda acceder a su correo de voz. SIP/IAX Password: Es la contraseña para el usuario (no la del administardor). Es similar a configurar una cuenta de correo, luego presionamos Save.

C. Configurar el buzon de voz Para configurar el buzon de voz accedemos por el menú izquierdo a VoiceMail.

En este debemos escribir en Extension for Checking messages el numero de buzón de voz, habilitando todos los check, también debemos configurar: Max greeting: el máximo tiempo de espera, en segundos. Maximum messages per folder: El máximo número de mensajes por folder. Max message time: La duración máxima del mensaje. Min message time: La duración minima del mensaje. Una vez configurado, presionamos Save. podemos ver un ejemplo de la interfaz en la imagen 11

IMPORTANTE: Una vez realizados todas las configuraciones debemos de aplicar los cambios, es decir el hecho de guardar cada configuración no significa que el servidor haya efectuado las operaciones, para ello subimos a la parte más alta del navegador damos click en Apply Changes

Diagramas

La propuesta incluye conectar via VPN a los campus de la Universidad Linda Vista. como se muestra en la imagen 5 nos podemos conectar desde calquier parte del mundo teniendo una conexión a Internet, asi como incluir en el servidor un servidor VoIP el cual podemos ver en la siguiente imagen: 6

Costos

Las licencias se describen abajo:

Hardware

Computadora. La computadora que se propone es de las siguientes caracteristicas: DELL Optiplex 780 Desktop

1. Procesador Intel® Core™2 Duo Processor E7500 (3M Cache, 2.93 GHz, 1066 MHz FSB)

2. Memoria 6GB de RAM Non-ECC dual-channel 1066MHz DDR3 SDRAM; ocupados 2 de 4 DIMMs soporta hasta 16GB max.

3. Disco Duro 500GB

4. Monitor: E190 Dell 19"LCD pantalla plana

5. Chipset Chipset Intel® Q45 Express con ICH10DO

6. Tarjeta de video Integrated Intel® Graphics Media Accelerator 45003

7. Conectividad LAN Ethernet® 10/100/1000 integrada Intel® 82567LM

8. Alimentación Desktop: 255W Standard PSU; ENERGY STAR® compliant, Active PFC

Software

El software que se usa es de licenciamiento gratuito y se enlistan a continuacion.

1. ubuntu server 12.04.2 : Es un sistema operativo basado en Linux y que se distribuye como software libre y gratuito

2. PPTPD: Es un software para servidor que ermite la administracion de un servidor VPN

3. webmin: Es una herramienta de configuración de sistemas accesible vía web para OpenSolaris, GNU/Linux y otros sistemas Unix

4. Asterisk: es un programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX)

5. FreepVx: FreePBX ofrece un interfaz GUI Html (interfaz gráfica de usuario) para administración de una central IP basada en Asterisk, muy fácil de usar pero con gran capacidad. También está basado en Open Source GPL.

CAPÍTULO IV

CONCLUSIÓN

En este trabajo se presentó una propuesta de una red privada virtual para la Universidad Linda Vista, procurando obtener los maximos beneficios para la misma al reducir el costo en la infraestructura de la Universidad. Tambien se pretende que se puedan reducir el uso de la telefonia convencional y migrar a la telefonía VoIP impactando directamente en el ahorro de presupuesto en las llamadas telefonicas en los planteles.

CAPÍTULO V

IMAGENES

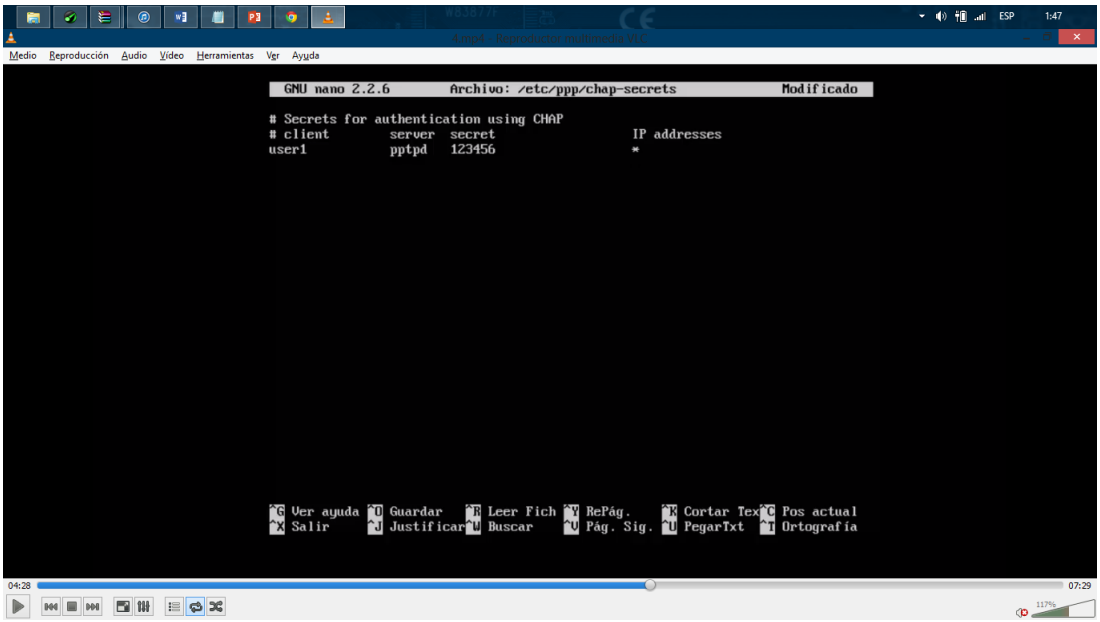

Figura 1. Añadiendo usuarios para servidor VPN

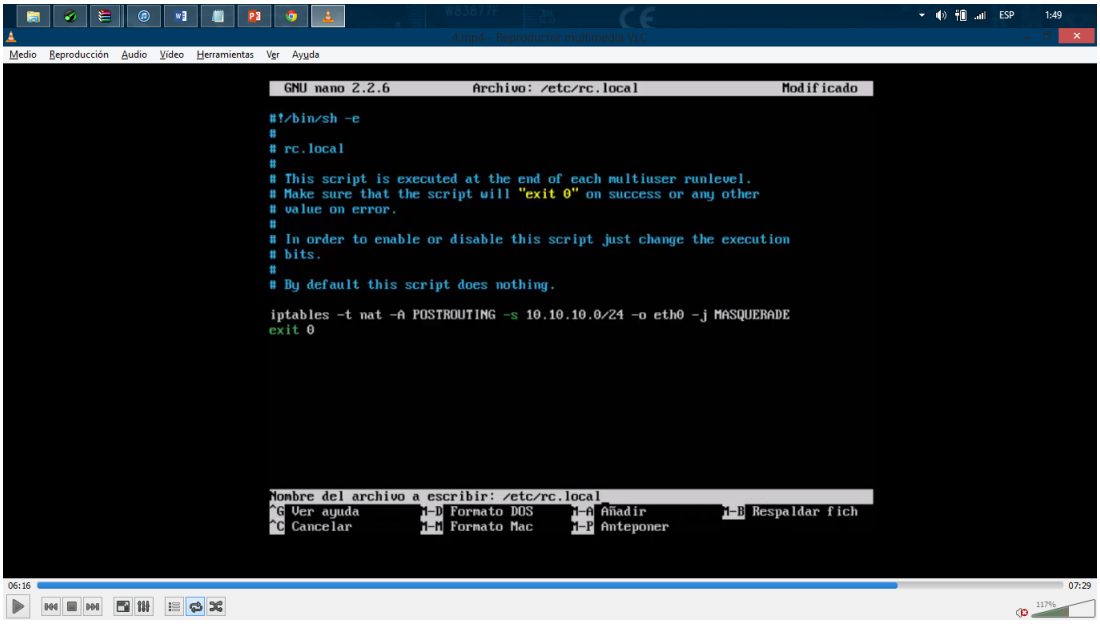

Figura 2. Modificando el script rc.local:

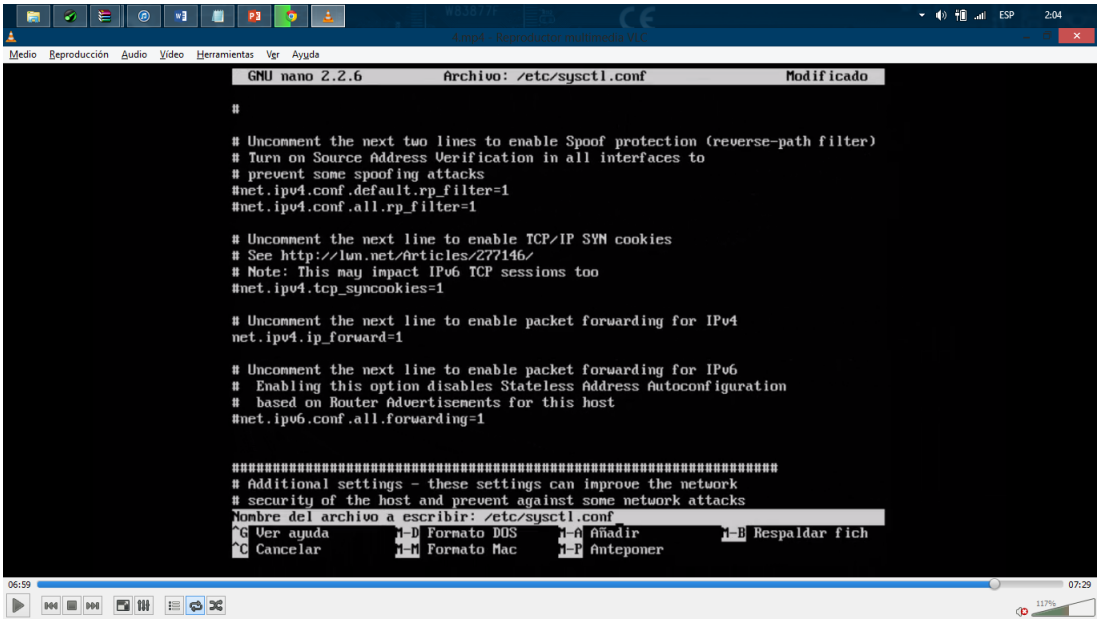

Figura 3. Modificando el script /etc/sysctl.conf:

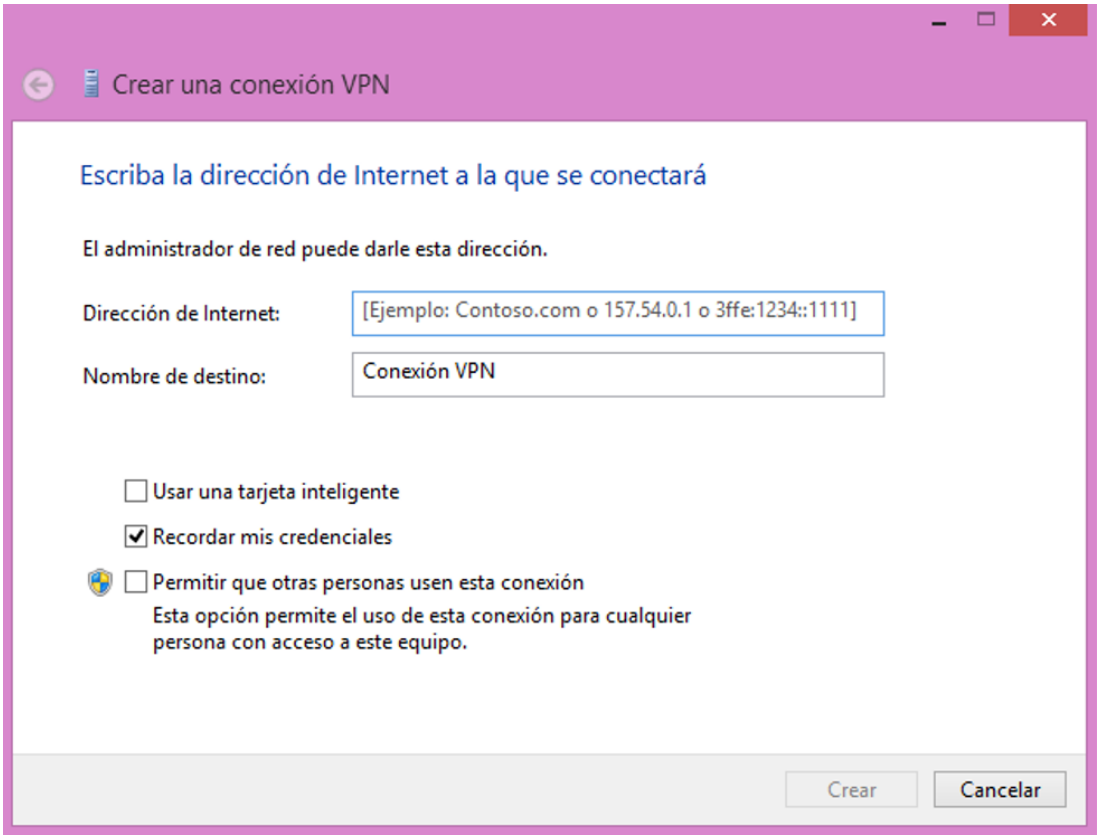

Figura 4. Conexion al servidor VPN: datos del seridor

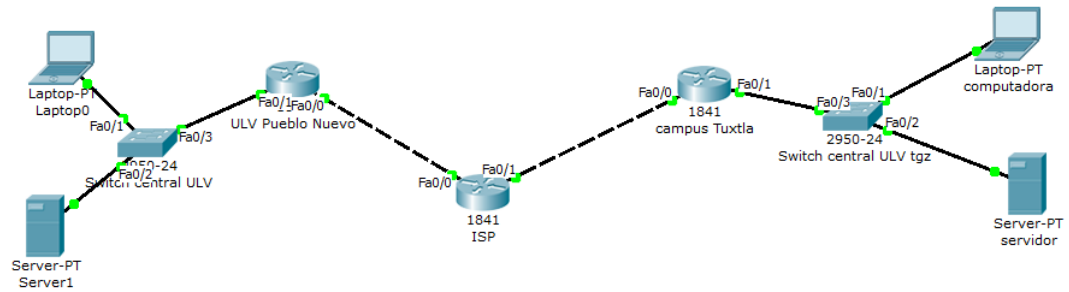

Figura 5. Diagrama de conexion

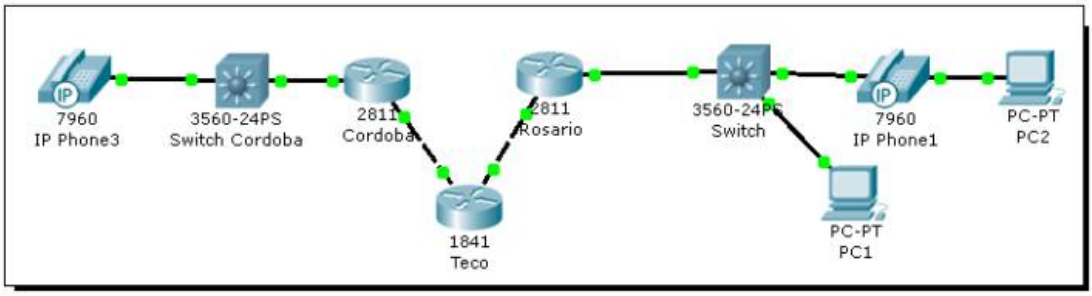

Figura 6. Diagrama de conexion de VoIP

```
  GNU nano 2.2.6        Archivo: /etc/asterisk/http.conf           Modificado

; configured directory.
;
;[post_mappings]
;
; In this example, if the prefix option is set to "asterisk", then using the
; POST URL: /asterisk/uploads will put files in /var/lib/asterisk/uploads/.
;uploads = /var/lib/asterisk/uploads/
;
enable = yes
bindaddr = 0.0.0.0
bindport = 8088
enablestatic = yes
redirect = / /static/config/index.html
[post_mappings]
backups = /var/lib/asterisk/gui_backups
moh = /var/lib/asterisk/moh
        _

^G Ver ayuda ^O Guardar   ^R Leer Fich ^Y RePág.    ^K Cortar Tex^C Pos actual
^X Salir     ^J Justificar^W Buscar    ^V Pág. Sig. ^U PegarTxt  ^T Ortografía
```

Figura 7. Ejemplo de configuracion de VoIP, el archivo http.conf

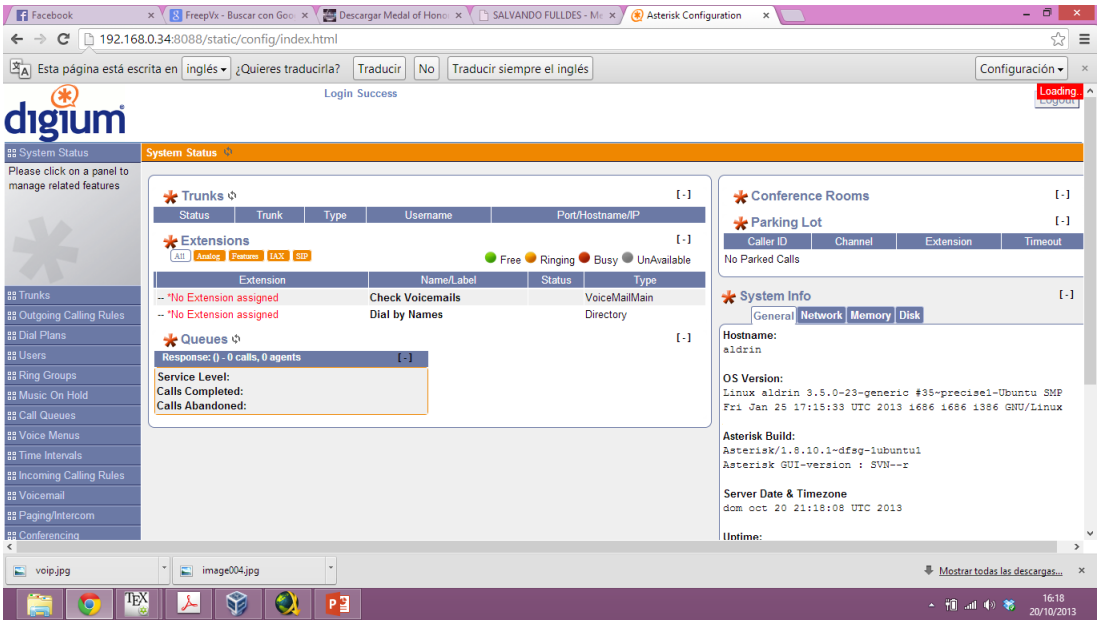

Figura 8. Captura de pantalla de FreepVx en la interfaz GUI HTML

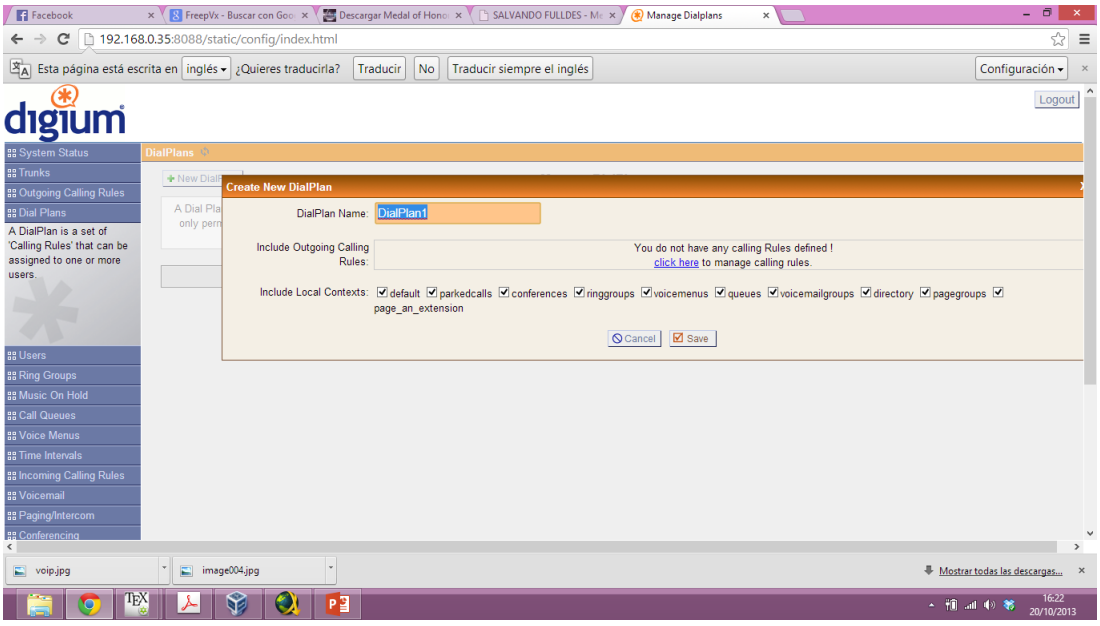

Figura 9. Captura de pantalla de FreepVx en la interfaz GUI HTML configurando un plan

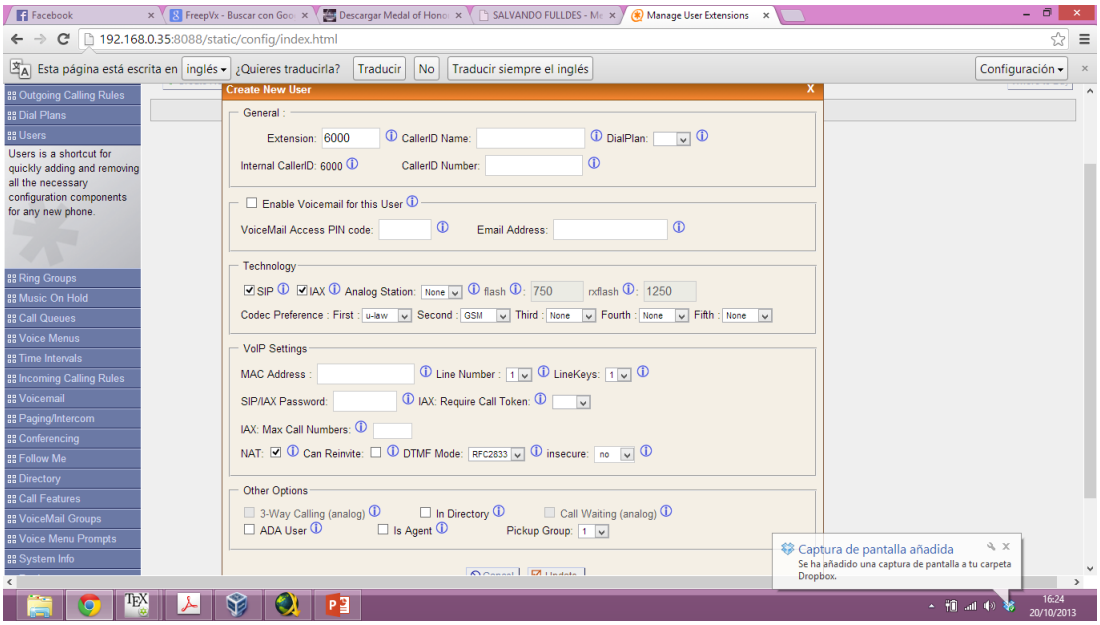

Figura 10. Captura de pantalla de FreepVx en la interfaz GUI HTML configurando un usuario

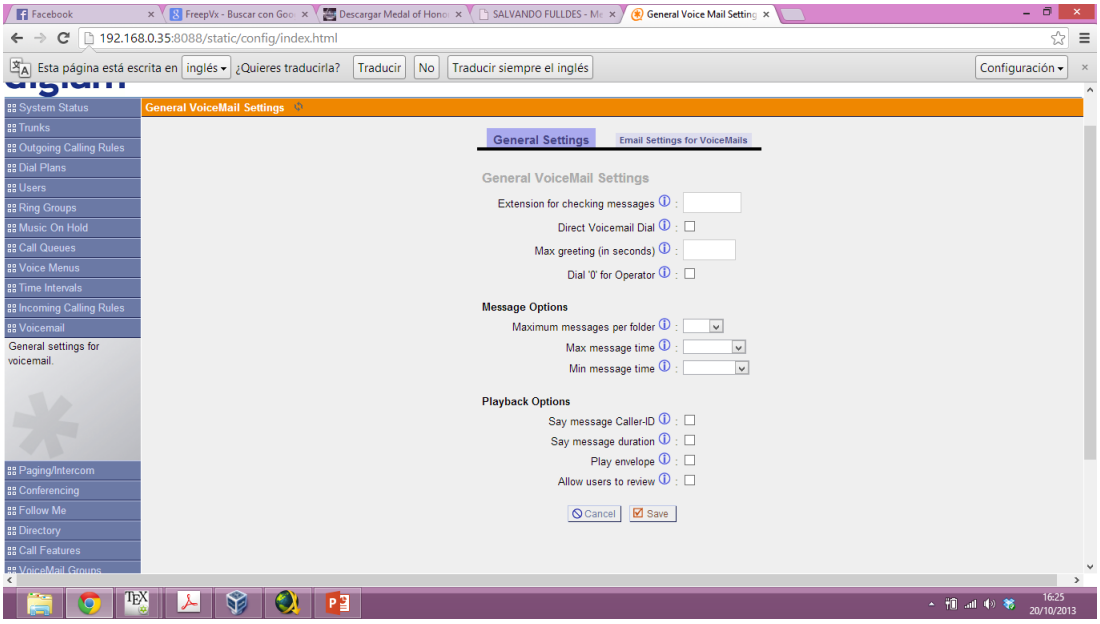

Figura 11. Captura de pantalla de FreepVx en la interfaz GUI HTML configurando el buzon de voz

LISTA DE REFERENCIAS

Brown, S. (2001). *Implementación de redes privadas virtuales*. McGraw-Hill Interamericana Editores, S.A. de C.V.

Caldas, E. A. B. (2007). Componentes básicos para una red segura bajo vpn. *Revista Inventum*, *1*(3), 36.

CISCO. (2006). *Configuración de multicast vpn extranet soporte.* Consultado el 04 de Diciembre 2006, en http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/extvpnsb.html

CISCO. (2013a). *Cisco vpn client.* Consultado el 09-25-2013, en http://www.lugro.org.ar/sites/default/files/introvpn.pdf

CISCO. (2013b). *Vpn.* Consultado el 25 de JULIO de 2013, en http://www.cisco.com/web/ES/solutions/es/vpn/index.html

Krause, J. (2013). *Microsoft directaccess = automatic vpn!* Consultado el 02-19-2013, en http://technet.microsoft.com/en-us/security/jj991832.aspx

Pena, T. F. (2013). *Ventajas de una vpn.* Consultado el 02-28-2008, en http://www.ac.usc.es/docencia/ASRII/Tema_4html/node19.html

Ramírez, A. M. (2013). *Estudio de tecnologias en conectividad segura y simulacion de la tecnologia ipsec para redes de comunicaciones.* Consultado el 09-25-2005, en http://www.publicaciones.urbe.edu/index.php/telematique/article/viewArticle/777/1871

Schmidt, J. (2001). *Seguridad en microsoft windows 2000* (1.ª ed.). Pearson Prentice Hall.

Shinder, D. (2004). *Comparar las opciones de vpn.* Consultado el 10 de junio 2004, en http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/VPN-Options.html

Shinder, D. (2013). *Comparing vpn options.* Consultado el 06-10-2004, en http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/VPN-Options.html

Víctor Hugo Taborda, C. A. D. (2004). *Comparar las opciones de vpn.* Consultado el 25 de julio 2013, en http://www.utp.edu.co/~victabo/TOPOLOGIA.htm