PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED DE UNIVERSIDADES DE SANTANDER (UNIRED) Y LA RED NACIONAL UNIVERSITARIA (RENATA), POR MEDIO DEL PROTOCOLO SIP, BASADOS EN HERRAMIENTAS DE CÓDIGO LIBRE

INGENIERO JUAN PABLO DÍAZ GÓMEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED DE UNIVERSIDADES DE SANTANDER (UNIRED) Y LA RED NACIONAL UNIVERSITARIA (RENATA), POR MEDIO DEL PROTOCOLO SIP, BASADOS EN HERRAMIENTAS DE CÓDIGO LIBRE.

INGENIERO JUAN PABLO DÍAZ GÓMEZ

MONOGRAFÍA PARA OPTAR AL TÍTULO DE
ESPECIALIZACIÓN EN TELECOMUNICACIONES

DIRECTOR:
INGENIERO FREDDY BELTRÁN

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

A mis Padres,
Hermanos y
Familiares

AGRADECIMIENTOS

Deseo expresar mi agradecimiento en primer lugar a DIOS que siempre ha estado en los momentos más difíciles de mis proyectos y en mi vida, también por darme unos padres maravillosos de quienes siempre he tenido el apoyo incondicional en cada paso que doy.

Quiero agradecer la ayuda, el tiempo y la confianza que en todo momento me ha brindado el director del proyecto Ing. Freddy Beltrán, quien ha tenido mucha paciencia, y que su único interés lo centró en trasmitirme todos sus conocimientos referentes al proyecto.

Agradezco a todos los docentes de la Especialización de Telecomunicaciones de la Universidad Industrial de Santander por todos sus aportes académicos durante toda la Especialización.

A las directivas de la Especialización de Telecomunicaciones por el soporte en todos los sentidos durante el tiempo de estancia, y a los tutores que estuvieron siempre presentes en el desarrollo de la Especialización.

No puedo dejar de agradecer a mi querida novia e Ingeniera Angélica María Montoya que gracias a su amistad, dedicación, apoyo y orientación me ayudo a realizar la monografía.

Y finalmente quiero agradecer a todas las personas que aunque no guiaron mi proyecto, estuvieron siempre presentes para despejar cualquier duda.

RECONOCIMIENTO

A la Universidad Industrial de Santander por su gran trayectoria y por su aporte educacional durante mi tiempo de estudio.

A la Especialización de Telecomunicaciones por recibirme y acogerme como alumnos de su proyecto educacional y por el soporte en todo los sentidos durante el tiempo de estancia.

CONTENIDO

pag

INTRODUCCIÓN *15*

JUSTIFICACIÓN *16*

OBJETIVO GENERAL *17*

OBJETIVOS ESPECÍFICOS *18*

ESTADO DEL ARTE *19*

1. TELEFONÍA *21*

1.1. PSTN – RTB **21**

1.2. PBX **22**

1.3. VoIP Y TELEFONIA IP **22**

1.3.1. VENTAJAS VoIP 23

1.3.2. LIMITACIONES VoIP 23

1.3.3. REQUERIMIEMTOS VoIP 24

1.4. QoS **24**

1.5. JITTER **24**

1.6. LATENCIA **25**

1.7. PERDIDAS DE PAQUETES **25**

1.8. ECO **25**

1.8.1. VALORES RECOMENDADOS: 26

1.8.2. POSIBLES SOLUCIONES: 26

1.9. ESTÁNDARES ABIERTOS Y CÓDIGO LIBRE **26**

2. HERRAMIENTAS DE SOFTWARE DE CÓDIGO LIBRE *29*

2.1. ASTERISK **29**

2.1.1. ARQUITECTURA DE ASTERISK 30

2.1.2. Módulos Cargables APIS: 31

2.1.3. CARACTERISTICAS DE ASTERSIK 33

2.1.4. CODECS 35

2.1.5. PROTOCOLOS 35

2.1.6. PATRONES DE MARCADO 37

2.1.7. EXTENSIONES RESERVADAS 37

3. ELASTIX *39*

4. TRIXBOX 40

5. RED VPN 41

5.1. NECESIDADES Y SURGIMIENTO DE LAS VPNS 41

5.2. ESTRUCTURA DE LAS VPNS 42

5.3. PROTOCOLOS UTILIZADOS EN LAS VPNS 45

5.3.1. PPTP 45

5.3.2. IPSEC 47

5.3.3. L2TP 50

5.4. CONFIGURACIÓN DE PROTOCOLOS 53

5.4.1. CONFIGURACIÓN DE UNA VPN BAJO WINDOWS 53

5.4.2. CONFIGURACIÓN DE UNA VPN BAJO LINUX 61

6. MIKROTIK 65

7. PROCEDIMIENTO PARA EFECTUAR VPN CON MIKROTIK 67

8. SOFTPHONE 71

9. NAT: Traducción de Direcciones de Red 72

9.1. DNAT: Destinantion-NAT 73

9.2. FIREWALL 74

9.2.1. MONOWALL 75

10. UNIRED 76

10.1. MIEMBROS DE UNIRED 76

10.2. CONECTIVIDAD 77

11. RENATA 78

11.1. MIEMBROS DE RENATA 78

11.2. CONECTIVIDAD 80

12. ACTIVIDADES 83

13. INSTALCIÓN BASICA PILOTO ENTRE LA EMPRESA BUSINESS STRATEGY LTDA DE GIRÓN Y LA SEDE DE TRABAJO DEL PROYECTO EN LA CIUDAD DE BUCARAMANGA. 87

13.1. PAQUETES REQUERIDOS PARA LA INSTALACIÓN DE LAS CENTRALITAS ASTERISK 88

13.2. INSTALACION DE LOS PAQUETES DE ASTERISK REQUERIDOS 89

13.3. ESQUEMA DE PRUEBAS DE CONEXIÓN ENTRE LA EMPRESA BUSINESS STRATEGY LTDA Y LA SEDE DE TRABAJO DEL PROYECTO. 92

13.4. CREACION DE EXTENSION TIPO SIP PARA LA COMUNICACION ENTRE LAS SECRETARIAS DE LA EMPRESA BUSINESS STRATEGY LTDA. Y LA SEDE DE TRABAJO DEL PROYECTO 93

13.5. DESARROLLO DEL PLAN DE DISCADO PARA NUESTRAS EXTENSIONES..... 95

13.6. CREACION DE LAS TRONCALES IAX PARA LA CONEXIÓN ENTRE LAS CENTRALTAS DE LA EMPRESA BUSINESS STRATEGY LTDA. Y LA SEDE DE TRABAJO DEL PROYECTO..... 97

13.7. CREACIÓN DEL IVR 99

13.7.1. PLAN DE MARCADO..... 99

13.8. CONFIGURACIÓN DEL SOFTPHONE (XLITE) PARA PERMITIR LAS LLAMADAS DESDE LA EMPRESA Y LA SEDE DEL PROYECTO. 100

14. DISEÑO DEL PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED DE UNIVERSIDADES DE SANTANDER (UNIRED) Y LA RED NACIONAL UNIVERSITARIA (RENATA) 103

14.1. COSTO DE DISEÑO DEL MODELO DE INFRAESTRUCTURA PARA LA INTERCONEXIÓN ENTRE LA RED UNIRED Y LA RED RENATA.....105

14.2. VENTAJAS DE LA IMPEMENTACIÓN DEL PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED (UNIRED) Y LA RED NACIONAL UNIVERSITARIA 107

15. RECOMENDACIONES..... 110

16. CONCLUSIONES..... 111

17. ANEXO SIP.CONF..... 113

18. BIBLIOGRAFIA..... 117

INDICE DE FIGURAS

pag

Figura 1 Arquitectura Asterisk.....30
Figura 2 Estructura VPN.....42
Figura 3 Capas del Encapsulamiento PPTP.....47
Figura 4 Marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local.....51
Figura 5 Relación entre los marcos PPP y los mensajes de control.....52
Figura 6 Red Local.....72
Figura 7 Esquema de Conectividad UNIRED.....77
Figura 8 Equipo UNIRED.....77
Figura 9 Mapa de Conexión.....82
Figura 10 Conexión entre la sede de Trabajo del Proyecto y La Empresa BS Ltda. 88
Figura 11 Diagrama de Conexión entre La Empresa Business Strategy Ltda. y la sede de Trabajo del Proyecto.....93
Figura 12 Diagrama de Conexión entre UNIRED y RENATA.....103

INDICE DE TABLA

pag

Tabla 1. Actividad No 1.....83
Tabla 2. Actividad No 2.....83
Tabla 3. Actividad No 3.....84
Tabla 4. Actividad No 4.....84
Tabla 5. Actividad No 5.....85
Tabla 6. Actividad No 6.....85
Tabla 7. Actividad No 7.....85
Tabla 8. Actividad No 8.....86
Tabla 9. Actividad No 9.....86
Tabla 10 Costo de Diseño 106

RESUMEN

1. TITULO

PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED DE UNIVERSIDADES DE SANTANDER (UNIRED) Y LA RED NACIONAL UNIVERSITARIA (RENATA), POR MEDIO DEL PROTOCOLO SIP, BASADOS EN HERRAMIENTAS DE CÓDIGO LIBRE[*]

2. AUTORES

Juan Pablo Díaz Gómez[**]

3. PALABRAS CLAVES

ASTERISK, RED VIRTUAL PRIVADA, TELEFONIA, VOZ SOBRE IP, CODIGOS, PROTOCOLO, FUENTES, HERRAMIENTAS, FIREWALL, MONOWALL, IAX, SIP, IVR, XLITE, PPP, PPTP.

4. DESCRIPCION

El proyecto consiste en elaborar un escenario de telecomunicaciones apropiado para la interconexión entre la red de Universidades del área Metropolitana de Bucaramanga UNIRED (UIS, USTA, UPB, UNAB, UDI, UDES, UNISANGIL, UNIPAZ, UTS, UMB, UCC, ICP, ADEL, UNIBOYACA Y UPTC.) a la red nacional Universitaria y centros de investigación del país RENATA por medio de voz sobre IP con el uso de herramientas de código libre (GNU), el cual permitirá el intercambio de información académica e investigativa y la futura proyección para la conexión con la red CLARA (Cooperación Latino Americana de Redes Avanzadas) y ALICE (América Latina Interconectada con Europa) que ayudará a extender fronteras con todas las redes internacionales de alta velocidad y los centros de investigación más desarrollados del mundo. Para el desarrollo del proyecto se hizo un análisis con las personas responsables de la red UNIRED, para averiguar en qué estado se encuentra la red actualmente en materia de tecnología y dispositivos existentes para así poder generar la documentación e información necesaria que nos permita una mejor contextualización del proyecto a diseñar. También se investigo todo acerca de la Red Privada Virtual, los diferentes protocolos involucrados en el diseño, los programas básicos en código libre y el sistema operativo Linux, también de los diferentes dispositivos de red y demás elementos de hardware necesarios para el diseño. Estos diferentes dispositivos y programas con sus respectivas configuraciones ayudarán al desarrollo del modelo que permitirá la conexión por medio de la telefonía IP de forma gratuita entre la red UNIRED y la red RENATA.

[*] Monografía

[**] Estudiantes Facultad de Ciencias Físico-Mecánica. Escuela de Ingeniería Electrónica. Director: Ing. Fredy Beltrán

ABSTRACT

1. TITLE

PROTOTYPE OF VOICE OVER IP INTERCONNECTION NETWORK BETWEEN THE UNIVERSITY OF SANTANDER (UNIRED) AND THE NATIONAL UNIVERSITY NETWORK (RENATA), THROUGH THE SIP PROTOCOL BASED ON OPEN SOURCE TOOLS[*].

2. AUTHORS

Juan Pablo Díaz Gómez[**]

3. KEYWORDS

ASTERISK, VPN, PSTN, VoIP, CODECS, PROTOCOL, SOURCE, TOOLS, FIREWALL, MONOWALL, IAX, SIP, IVR, XLITE, PPP, PPTP.

4. DESCRIPCION

The project is to develop an appropriate telecommunications scenario for the interconnection between the network of Universities of the Metropolitan Area of Bucaramanga UNIRED (UIS, USTA, UPB, UNAB, UDI, UDES, UNISANGIL, UNIPAZ, UTS, UMB, UCC, ICP, ADEL , UNIBOYACA And UPTC.) to the national university and research centers in the country RENATA through voice over IP using open source tools (GNU), which allow the exchange of academic information and research and the future projection for network connection CLARA (Latin American Cooperation of Advanced Networks) and ALICE (Latin America Interconnected with Europe) that will help extend borders with all high speed international networks and research centers world's most developed. For the development of the project was also done with people UNIRED network managers to find out what state the network is currently on existing technology and devices so you can generate documentation and information necessary to enable us to better contextualize design project.Also was investigated about the Virtual Private Network, the various protocols involved in the design, basic programs and the open source Linux operating system, also from the various network devices and other necessary elements for design. These various devices and programs with their respective configurations will help the development of the model that will allow connection via IP telephony for free between the network and the network UNIRED RENATA.

[**] Student of faculty of physic-mechanical sciences. Electronic engineering school. Director: Ing. Fredy Beltran

INTRODUCCIÓN

La finalidad del proyecto es el diseño de un escenario de telecomunicaciones apropiado para la interconexión entre la red de Universidades del área Metropolitana de Bucaramanga UNIRED (UIS, USTA, UPB, UNAB, UDI, UDES, UNISANGIL, UNIPAZ, UTS, UMB, UCC, ICP, ADEL, UNIBOYACA Y UPTC.) a la red nacional Universitaria y centros de investigación del país RENATA por medio de voz sobre IP con el uso de herramientas de código libre (GNU), el cual permitirá el intercambio de información académica e investigativa y la futura proyección para la conexión con la red CLARA (Cooperación Latino Americana de Redes Avanzadas) y ALICE (América Latina Interconectada con Europa) que ayudará a extender fronteras con todas las redes internacionales de alta velocidad y los centros de investigación más desarrollados del mundo.

Para el desarrollo del proyecto se debe hacer un análisis con las personas responsables de la red UNIRED, para averiguar en qué estado se encuentra la red actualmente en materia de tecnología y dispositivos existentes para así poder generar la documentación e información necesaria que nos permita una mejor contextualización del proyecto a diseñar. También es necesario averiguar todo acerca de la Red Privada Virtual, los diferentes protocolos involucrados en el diseño, los programas básicos en código libre y el sistema operativo Linux, también de los diferentes dispositivos de red y demás elementos de hardware necesarios para el diseño. Estos diferentes dispositivos y programas con sus respectivas configuraciones ayudarán al desarrollo del modelo que permitirá la conexión por medio de la telefonía IP de forma gratuita entre la red UNIRED y la red RENATA.

JUSTIFICACIÓN

Actualmente, el increíble adelanto de Internet y de las Tecnologías de la Información y de las Comunicaciones han permitido que la educación no se quede atrás y ha encontrado en esta maravilla una oportunidad de progreso. De esta manera, se ha permitido romper con las restricciones que tienen las diferentes Universidades de poder estar en contacto mutuo y así mismo con los estudiantes, pudiendo obtener un mejor desarrollo educativo y personal en general.

El desarrollo del proyecto es fundamental para obtener un gran avance en la ayuda educacional e investigativa para los estudiantes así como en lo tecnológico para las diferentes Universidades de Bucaramanga, manejando la facilidad de comunicación entre ellas y con la red nacional de Universidades y centros investigativos de manera rápida, eficaz, utilizando una plataforma basada en voz

OBJETIVO GENERAL

Diseñar un modelo de infraestructura de red de telecomunicaciones para la implementación de una Plataforma de Voz sobre IP que permitirá la interconexión de la red de Universidades del área Metropolitana de Bucaramanga UNIRED (UIS, USTA, UPB Y DEMAS…) con la red nacional Universitaria y centros de investigación RENATA por medio de código libre.

OBJETIVOS ESPECÍFICOS

- Investigar y profundizar sobre las diferentes herramientas de software de código libre que se utilizan en el mercado, sobre la red VPN, los protocolos involucrados en el diseño y los diferentes dispositivos de hardware que serán implementados en la plataforma de voz sobre IP que ayudará a establecer la interconexión entre la red UNIRED y la red RENATA.

- Analizar cómo se encuentra la infraestructura de la red UNIRED y RENATA para obtener información importante para el desarrollo del proyecto.

- Estudiar la configuración de las diferentes herramientas de software y hardware a utilizar para el diseño e instalar una estructura básica piloto para la generación de pruebas y así poder observar el funcionamiento de la plataforma. Creando así un documento guía, que permitirá servir de aporte o asistente para posteriores implantaciones por los administradores de red de las nuevas Entidades Universitarias que quieran adherirse a este modelo de VoIP en la red UNIRED y en la red Nacional Universitaria.

- Diseñar el modelo para la interconexión de la red de Universidades del Área Metropolitana de Bucaramanga con la red nacional de Universidades y centros de investigación del país.

ESTADO DEL ARTE

[1]Hace 30 años Internet no existía, y las comunicaciones se realizaban por medio del teléfono a través de la red telefónica pública conmutada (PSTN), pero con el pasar de los años y el avance tecnológico han aparecido nuevas tecnologías y aparatos bastante útiles que permiten pensar en nuevas tecnologías de comunicación como son los PCS, teléfonos celulares y finalmente la popularización de la gran red Internet.

Hoy por hoy podemos ver una gran revolución en comunicaciones ya que todas las personas usan los computadores e Internet en el trabajo y en el tiempo libre para comunicarse con otras personas, para intercambiar datos y a veces para hablar con personas usando aplicaciones como NetMeeting o teléfono IP (Internet Phone), el cual particularmente comenzó a difundir en el mundo la idea que en el futuro se podría utilizar una comunicación en tiempo real por medio del PC como es VoIP (Voice Over Internet Protocol).

Después de haber constatado que desde un PC con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, una institución que disponga de una red de datos y que tenga un ancho de banda bastante grande, se pensaría en la utilización de esta red para el tráfico de voz entre las distintas áreas de la institución como de instituciones vecinas. Las ventajas que se obtendrían al utilizar la red para transmitir tanto la voz como los datos son evidentes, ahorro de costos de comunicaciones, pues las llamadas entre las distintas áreas de la empresa saldrían gratis.

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP, no podía hacerse esperar. La aparición del VoIP junto con los bajos precios de los DSP's (procesador digital de señal), los cuales son claves en la compresión y

descompresión de la voz. Son los elementos que han hecho posible el despegue de estas tecnologías.

Por último vale aclarar que en junio de 2004 el Ministerio de Comunicaciones de Colombia publicó el documento titulado VoIP, ("Borrador para discusión, no compromete la posición oficial del Ministerio de Comunicaciones de Colombia") en el que se intenta mostrar el panorama técnico y legal existente con el objetivo fundamental de "hacer un llamado al sector para abrir el debate … dado que su aplicación posiblemente obligaría a cambiar la regulación vigente en aspectos tan importantes como el modelo tarifario, régimen de interconexión, régimen de competencia, habilitaciones y obligaciones entre otros."

Si bien se anunciaba para el 8 de octubre de 2004 la expedición de un Documento de política definitivo y plan de acción, hasta la fecha no ha sido expedida norma alguna en la materia, y tampoco ha aparecido algún nuevo pronunciamiento oficial de parte de la entidad estatal. De cualquier forma, desde hace pocos meses si se ha empezado a conocer la promoción y publicidad abiertas al público en general de servicios de telefonía IP, por parte de algunos de los principales competidores del servicio de telefonía de larga distancia en el mercado nacional (Orbitel y ETB entre otros).

[1]*Guía de redacción: Artículo en Monografia.com y Ministerio de Comunicaciones

CAPITULO I

1. TELEFONÍA

La telefonía fija o convencional es aquella que hace referencia a las líneas y equipos que se encargan de la comunicación entre terminales telefónicos no portables y generalmente enlazados entre ellos con la central por medio de conductores metálicos.

Existen casos particulares en telefonía fija en los que la conexión con la central se hace por medios radioeléctricos, como es el caso de la telefonía rural mediante acceso celular, en la que se utiliza parte de la infraestructura de telefonía móvil para facilitar servicio telefónico a zonas de difícil acceso para las líneas convencionales de hilo de cobre. No obstante estas líneas a todos los efectos se consideran como de telefonía fija.

1.1. PSTN – RTB

PSTN es la Red Pública Telefónica Conmutada (Public Switched Telephone Network), “la red de redes telefónicas” o más conocida como “la red telefónica.” En castellano la PSTN es conocida como la red pública conmutada (RTC) o red telefónica básica (RTB). De la misma forma que Internet es la red global IP, la RTB es la amalgama de todas las redes conmutadas de teléfono. Una diferencia muy importante entre la RTB e Internet es la noción de “flujo de información”. En telefonía los flujos de información son cada una de las llamadas o conversaciones mientras que en Internet es cada uno de los paquetes de datos. Si una conversación se efectúa en una RTB se tiene que reservar un canal (circuito) dedicado de 64 Kbps, pero en Internet la misma conversación puede coexistir con otros servicios de manera simultánea. La RTB ha estado históricamente

gobernada por estándares creados por la UIT, mientras que Internet es gobernada por los estándares del IETF. Ambas redes, la RTB e Internet usan direcciones para encaminar sus flujos de información. En la primera se usan números telefónicos para conmutar llamadas en las centrales telefónicas, en Internet se usan direcciones IP para conmutar paquetes entre los enrutadores (routers).

1.2. PBX

Acrónimo de Private Branch eXchange o Private Business eXchange.

Es una central telefónica que es utilizada para negocios privados. Una central telefónica es el lugar (puede ser un edificio, un local o un contenedor), utilizado por una empresa operadora de telefonía, donde se albergan el equipo de conmutación y los demás equipos necesarios, para la operación de llamadas telefónicas en el sentido de hacer conexiones y retransmisiones de información de voz. En este lugar terminan las líneas de abonado, los enlaces con otras centrales y, en su caso, los circuitos interurbanos necesarios para la conexión con otras poblaciones.

El uso de un PBX es para conecta todos los teléfonos de una empresa de manera separada a la red de telefonía local pública PSTN. Las llamadas hacia afuera en un PBX son hechas marcando un número (generalmente 9 o 0) seguido del número externo, entonces una línea troncal es seleccionada automáticamente y sobre ésta se completa la llamada.

1.3. VoIP Y TELEFONIA IP

Ambos conceptos tienen un significado distinto, aunque la mayoría de las veces hacemos referencia como si se tratara de lo mismo.

VoIP es una Técnica que permite digitalizar la voz para luego enviarla sobre paquetes IP a través de la red de datos.

Telefonía IP, son servicios de valor agregado que utilizan VoIP como herramienta para el tratamiento de la voz. Por ejemplos de telefonía IP encontramos inicialmente los mismos servicios que en la telefonía tradicional (buzón de voz, IVR, enrutamiento de llamadas, etc.) pero con la diferencia que el medio de comunicación es la red de datos.

Las alternativas tecnológicas de VoIP se pueden dividir de una manera sencilla en dos grandes grupos: tecnologías cerradas-propietarias y sistemas abiertos. En el primer grupo de tecnologías nos encontramos con el conocido Skype o el ya legendario Cisco Skinny (SCCP). En el segundo grupo de tecnologías nos encontramos con los estándares abiertos basados en SIP, H.323 o IAX.

1.3.1. VENTAJAS VoIP

- ✓ Ahorro de ancho de banda y aprovechamiento de los intervalos entre ráfagas de datos haciendo un uso más efectivo de canales costosos.
- ✓ Convergencia de las comunicaciones de datos y voz en una plataforma única, facilitando la gestión, el mantenimiento y el entrenamiento del personal.
- ✓ Facilidad de incorporar servicios especiales.

1.3.2. LIMITACIONES VoIP

- ✓ Las redes IP normalmente no permiten garantizar un tiempo mínimo para cruzarlas.
- ✓ Las redes IP están diseñadas para descartar paquetes en caso de congestión y retransmitirlos en caso de error. Esto no es adecuado para la voz.
- ✓ Los retardos de cientos de ms, comunes en redes de datos, son inaceptables en una conversación telefónica.

1.3.3. REQUERIMIEMTOS VoIP

- ✓ Utilizar protocolos que permitan garantizar cierto grado de calidad de servicio (QoS) y no utilicen retransmisiones. Prioridad a la voz sobre los datos.
- ✓ Controlar el número máximo de saltos y los demás factores que contribuyen al retardo de transmisión para mantenerlo por debajo de 170 ms.

1.4. QoS

Las tecnologías de QoS (Quality of Service, Calidad de Servicio) garantizan que se transmitirá cierta cantidad de datos en un tiempo dado (throughput).
Una red IP está basada en el envió de paquetes de datos, estos paquetes de datos tienen una cabecera que contiene información sobre el resto del paquete. Existe una parte del paquete que se llama TOS, en realidad esta parte está pensada para llevar banderas o marcas. Lo que se puede hacer para darle prioridad a un paquete sobre el resto es marcar una de esas banderas (flags).

1.5. JITTER

Jitter se refiere a cómo de variable es la latencia en una red. Un elevado valor de Jitter, más de 50 msec, ocasiona incrementos de latencia y de pérdida de paquetes. Al hablar con alguien es importante que oigan lo que decimos en el mismo orden que lo dijimos, de otra forma no entenderán lo que estamos diciendo. Para corregir estos efectos de Jitter, los puntos finales de Voz ip recogen los paquetes en un buffer (buffer jitter) y los ponen de nuevo juntos sincronizados y en el orden correcto antes que el receptor los oiga. Aunque este procedimiento funciona, se ha de realizar de forma balanceada. Procesar ese buffer añade retardo a la llamada, y a más buffer, más retardo. También debemos tener

presente que el buffer es finito. Si los paquetes de Voz IP llegan cuando el buffer está lleno, se perderán y el receptor nunca los oirá.

1.6. LATENCIA

En redes informáticas de datos se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

- Otros factores que influyen en la latencia de una red son:

- ✓ El tamaño de los paquetes transmitidos.
- ✓ El tamaño de los buffers dentro de los equipos de conectividad. Ellos pueden producir un Retardo Medio de Encolado.

1.7. PERDIDAS DE PAQUETES

La pérdida de paquetes está definida como el porcentaje de paquetes perdidos en una transmisión. Lo contrario a la perdida de paquetes es la cantidad de paquetes recibidos, la cual se define como el complemento de la pérdida de paquetes, es decir 100 menos el porcentaje de pérdida de paquetes.

1.8. ECO

El eco se produce por un fenómeno técnico que es la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el micrófono. El eco también se suele conocer como reverberación.

*El eco se define como una reflexión retardada de la señal acústica original***.**

El eco es especialmente molesto cuanto mayor es el retardo y cuanto mayor es su intensidad con lo cual se convierte en un problema en VoIP puesto que los retardos suelen ser mayores que en la red de telefonía tradicional.

1.8.1. VALORES RECOMENDADOS:

El oído humano es capaz de detectar el eco cuando su retardo con la señal original es igual o superior a 10 ms. Pero otro factor importante es la intensidad del eco ya que normalmente la señal de vuelta tiene menor potencia que la original. Es tolerable que llegue a 65 ms y una atenuación de 25 a 30 dB.

1.8.2. POSIBLES SOLUCIONES:

En este caso hay dos posibles soluciones para evitar este efecto tan molesto.

- **Supresores de eco** - Consiste en evitar que la señal emitida sea devuelta convirtiendo por momentos la línea full-dúplex en una línea half-dúplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario. El tiempo de conmutación de los supresores de eco es muy pequeño. Impide una comunicación full-dúplex plena.

- **Canceladores de eco** - Es el sistema por el cual el dispositivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido). El dispositivo filtra esa información y cancela esas componentes de la voz. Requiere mayor tiempo de procesamiento.

1.9. ESTÁNDARES ABIERTOS Y CÓDIGO LIBRE

No podríamos estar hablando de la libertad de construir una red telefónica sin la existencia de los estándares abiertos y el código libre. Los estándares abiertos permiten que cualquiera pueda implementar un sistema con garantías de interoperabilidad. Gracias a esa interoperabilidad no sólo podemos crear una red telefónica sino que, además, podemos conectarla a la red telefónica global. Con el

código libre podemos aprender de experiencias parecidas, integrar sus soluciones y compartir nuestros propios resultados con los demás.
Para ser conscientes de la importancia de los estándares abiertos quizás sea bueno empezar presentando una definición de “estándar.” Un estándar es un conjunto de reglas, condiciones o requerimientos que describen materiales, productos, sistemas, servicios o prácticas. En telefonía, los estándares garantizan que todas las centrales de telefonía sean capaces de operar entre sí. Sin ese conjunto de reglas comunes un sistema de telefonía de una región sería incapaz de intercambiar llamadas con otro que esté, tan sólo, unos kilómetros más allá.

Aunque muchos de los estándares de telefonía son públicos, los sistemas siempre han estado bajo el control de un grupo muy limitado de fabricantes. Los grandes fabricantes de sistemas de telefonía son los únicos capaces de negociar contratos a nivel regional o incluso nacional.

Ésta es la razón que puede explicar porqué es muy común encontrar siempre el mismo tipo de equipos a lo largo de un mismo país.

Los equipos de telefonía tradicionales, además, tienen la particularidad de haber sido diseñados para realizar un conjunto de tareas muy concretas. Normalmente, son equipos informáticos con aplicaciones muy específicas. Aunque las reglas que gobiernan la telefonía (los estándares) son relativamente abiertas, no es el caso de los equipos informáticos que los implementan. Al contrario de los estándares, el funcionamiento interno siempre se mantiene en secreto.

Dentro de la “poción mágica de la telefonía” los estándares abiertos son un ingrediente necesario, pero lo que realmente ha permitido esta nueva “revolución” ha sido la posibilidad de emular la funcionalidad de los sistemas de telefonía tradicionales con un programa funcionando en un ordenador personal. Todos los elementos necesarios están a tu alcance:

- ✓ tienes el acceso a los programas y a los equipos que permiten el intercambio de conversaciones telefónicas.
- ✓ tienes una red abierta y pública para intercambiar esas llamadas (la Internet).
- ✓ tienes la posibilidad de modificar cada uno de los elementos para adaptarlos a tus propias necesidades.

2. HERRAMIENTAS DE SOFTWARE DE CÓDIGO LIBRE

En estos momentos el software de código libre más utilizado es conocido con el nombre de ASTERISK aunque se maneja otro software llamado ELASTIX que en estos momentos es un programa reciente.

El programa utilizado para el desarrollo de la plataforma de voz sobre IP es ASTERISK, este programa nos permite una excelente configuración y mejor instalación de la central telefónica (IP-PBX).

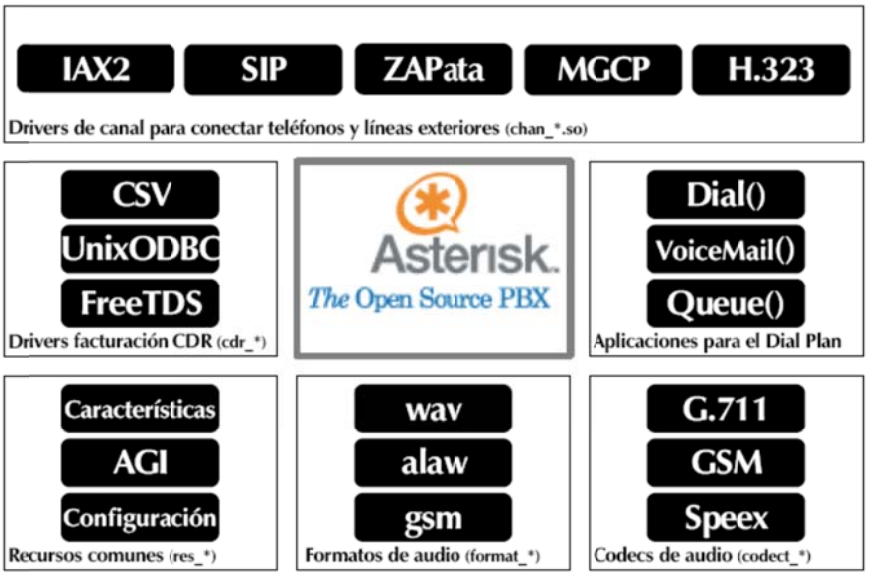
2.1. ASTERISK

Asterisk es una aplicación software libre de una central telefónica (IP-PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios. Su administración y gestión se realiza en modo consola vía comandos de texto. Pero existes aplicaciones que permiten realizar su configuración en forma grafica vía web. Asterisk tiene licencia GPL.
Asterisk es desarrollado mayoritariamente por la empresa estadounidense DIGIUM de la cual Mark Spencer es su fundador. Se ejecuta en sistemas de hardware estándares (arquitectura x86, x86_64, ppc) bajo GNU/Linux, BSD, MacOSX, Solaris y hasta Windows.

La primera Versión estable fue Asterisk 1.0 que fue publicada en el 2004. En Noviembre de 2005 es publicada Asterisk 1.2 con grandes mejoras sobre su predecesor. La última versión a la fecha, es Asterisk 1.4.4, liberada en Abril de 2007. En la actualidad es una solución probada y robusta, tanto para empresas que lo utilizan en funciones de PBX de uso interno como para grandes carriers e ITSP.

La recomendación de la capacidad para la instalación de una IPBX de no más de 5 extensiones es como mínimo, un Pentium III con 500MHZ y 256 megas de RAM, de 5 a 10 extensiones es de 1 GHz de procesador y 512 megas de RAM, hasta 25 extensiones es un procesador de 3 GHz y 1 GB de RAM y para más de 25 extensiones se maneja dos o más CPU's) en una arquitectura distribuida.

2.1.1. ARQUITECTURA DE ASTERISK



Asterisk esta cuidadosamente desarrollado para máxima flexibilidad. Está conformado por API`s específicas definidas alrededor de un núcleo central de PBX. Este núcleo avanzado maneja interconexión interna del PBX, abstraídos limpiamente por protocolos específicos, Codecs, e interfaces de hardware de aplicaciones de telefonía. Esto le permite al Asterisk utilizar cualquier hardware conveniente y tecnología disponible, ahora ó en el futuro para realizar sus funciones esenciales, conectando hardware y aplicaciones.

El Asterisk maneja internamente:

- ✓ **PBX SWITCHING:** La esencia del Asterisk, por supuesto es un sistema de conmutación de intercambio de rama privada (PXB), conectando llamadas entre varios usuarios y tareas automatizadas. La base de conmutación conecta a los usuarios llegando a varios software y hardware de interface.

- ✓ **LANZADOR DE APLICACIONES:** Lanza aplicaciones que mejoran servicios para usos tales como, voicemail, file playback y lista de directorio.
- ✓ **TRADUCTOR DE CODECS:** usa módulos de Codecs para codificar y decodificar varios formatos de comprensión de audio usado en la industria de la telefonía. Un gran número de Codecs están disponibles para satisfacer necesidades y llegar al mejor balance entre la calidad del audio.

- ✓ **ORGANIZADOR Y MANEJADOR:** Maneja organización de tareas de bajo nivel y sistemas de manejo para un óptimo performance bajo cualquier condición de carga.

2.1.2. Módulos Cargables APIS:

Cuatro APIs están definidos por módulos cargables, facilitando el hardware y la abstracción del protocolo. Usando este sistema APIs, la base del Asterisk no tiene que preocuparse de detalles como por ejemplo: que llamada está entrando o que Codecs está usando actualmente, etc.

- ✓ **CANAL API:** El canal API maneja el tipo de conexión al cual el cliente está llegando, sea una conexión VoIP, ISDN, PRI, o alguna otro tipo de tecnología. Módulos dinámicos son cargados para manejar los detalles más bajos de la capa de estas conexiones.

- ✓ **APLICACIÓN API:** Esta aplicación permite a varios módulos de tareas cumplir varias funciones, conferencias, paging, lista de directorios, voice mail en la línea de transmisión de datos, y cualquier otra tarea la cual PBX sea capaz de cumplir ahora o en el futuro son manejados por estos módulos.

- ✓ **TRADUCTOR DEL CODEC API:** Cargar módulos codecs para apoyar varios tipos de audio, codificando y decodificando formatos tales como GMS, mu law, a law, e incluso mp3.
- ✓ **FORMATO DE ARCHIVO API:** Maneja la lectura y escritura de varios formatos de archivos para el almacenaje de datos en el sistema de archivos.

Usando estos APIs Asterisk alcanza una completa abstracción entre sus funciones básicas como un servidor de sistema PBX y la variedad tecnológica existente (o en desarrollo) en el área de la telefonía.

La formula modular es lo que le permite al Asterisk integrar hardware de telefonía implementados y tecnología de paquetes de voz emergentes hoy en día.

La aplicación API provee el flexible uso de aplicaciones modulares para realizar cualquier acción flexible en demanda, también permite un desarrollo abierto de nuevas aplicaciones para satisfacer necesidades o situaciones únicas.

En conclusión, cargar todo el uso como módulos permite un sistema flexible, permitiéndole al administrador diseñar la mejor y más satisfactoria trayectoria para los usuarios en el sistema PBX y también modificar la trayectoria de llamadas para satisfacer las cambiantes necesidades de la comunicación que nos concierne.

2.1.3. CARACTERISTICAS DE ASTERSIK

El Asterisk basado en soluciones de telefonía ofrece un variado y flexible set de características (o menú).

Características de Llamadas

- ✓ ADSI en el menú de pantalla
- ✓ Receptor de alarma
- ✓ Añade mensajes
- ✓ Asistente automatizado
- ✓ Autentificación
- ✓ Listas negras
- ✓ Transfer oculto
- ✓ Grabado de llamadas detallado
- ✓ Llamada en ocupado
- ✓ Llamada entrante en no responder
- ✓ Llamada entrante variable
- ✓ Monitoreo de llamadas
- ✓ Estacionamiento de llamadas
- ✓ Llamadas en espera
- ✓ Grabación de llamadas
- ✓ Recuperación de llamadas
- ✓ Guía de llamadas (DID y ANI)
- ✓ Call snooping
- ✓ Transferencia de llamadas
- ✓ Llamadas en espera
- ✓ Identificación de usuarios
- ✓ Bloque de identificaron de usuarios
- ✓ Identificación de usuarios en llamadas de espera

- ✓ Tarjetas de llamadas
- ✓ Conferencias
- ✓ Recuperación de base de datos almacenados
- ✓ Integración de base de datos
- ✓ Dial por nombre
- ✓ Acceso directo al sistema interno
- ✓ No molestar
- ✓ e911
- ✓ ENUM
- ✓ Fax transmitidos y recibidos
- ✓ Lógica flexible de la extensión
- ✓ Lista de directorio interactivo
- ✓ Respuesta de voz interactivo
- ✓ Agentes de llamada local y lejana
- ✓ Macros
- ✓ Creación de música
- ✓ Transferencia de música
- o sistema básico de mp3
- o juegos al azar o en línea
- o control de volumen
- ✓ Privacidad
- ✓ Establecimiento de protocolo abierto (OSP)
- ✓ Paginación arriba
- ✓ Conversión de protocolo
- ✓ Recepción de llamadas lejanas
- ✓ Apoyo a oficinas de lejos
- ✓ Extensiones roaming
- ✓ Mensajes SMS
- ✓ Acceso a los medios afluyentes
- ✓ Transfer supervisado

- ✓ Detección de conversaciones
- ✓ 3 formas de llamadas
- ✓ Hora y fecha
- ✓ Transcodificación
- ✓ Trunking
- ✓ Entradas al VoIP
- ✓ Voicemail
- o indicador visual para los mensajes en espera
- o voicemails a emails
- o grupos de voicemail
- o interfaces de web voicemail

2.1.4. CODECS

- ✓ G.711 ulaw (usado en EUA) – (64 Kbps).
- ✓ G.711 alaw (usado en Europa y Brasil) – (64 Kbps)
- ✓ G.723.1 – Modo Passtrough
- ✓ G.726 32 Kbps en Asterisk 1.0.3 16/24/32/40 Kbps
- ✓ G.729 – Precisa Adquisición de licencia, a menos que este siendo usado en modo passthru (8 Kbps).
- ✓ GSM – (12 – 13 Kbps)
- ✓ iLBC – (15 Kbps)
- ✓ LPC10 – (2.5 Kbps)
- ✓ Speex – (2.15 44.2Kbps)

2.1.5. PROTOCOLOS

- ✓ IAX (intercambio del Asterisk). Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX. El protocolo IAX ahora se refiere generalmente al IAX2, la

segunda versión del protocolo IAX. El protocolo original ha quedado obsoleto en favor de IAX2. El principal objetivo de IAX ha sido minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red IP, con particular atención al control y a las llamadas de voz y suministrando un soporte nativo para ser transparente a NAT.

- ✓ H.323. Es un conjunto de normas para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable.

- ✓ SIP (sesión de inicio del protocolo). Session Initiation Protocol es un protocolo de control y señalización usado mayoritariamente en los sistemas de Telefonía IP, que fue desarrollado por el IETF (RFC 3261). Dicho protocolo permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y sus mayores ventajas recaen en su simplicidad y consistencia.

- ✓ MGCP (Media Gateway Control Protocol). Es un protocolo interno de señalización y control de VoIP cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente-servidor.

- ✓ SCCP (Cisco Skinny). Protocolo propietario usado entre el Cisco Call Manager y teléfonos IP Cisco. El Asterisk viene con un canal del sccp llamado skinny que se utiliza con los teléfonos de Cisco.

2.1.6. PATRONES DE MARCADO

Las reglas de marcado son muy importantes, y simples de aprender. Le indica al servidor cómo van a ser marcadas las llamadas en esta troncal. Puede ser utilizado para agregar ó quitar prefijos. Los números que no tengan una equivalencia con ningún patrón definido, serán marcados como estén.

Reglas:

- ✓ X Equivale a cualquier dígito de 0 a 9
- ✓ Z Equivale a cualquier dígito de 1 a 9
- ✓ N Equivale a cualquier dígito de 2 a 9
- ✓ [1,5-9] Equivale a cualquier dígito ó letra entre llaves (en este ejemplo 1,5, 6,7, 8, 9)
- ✓ . Equivale a uno ó más caracteres (no permitido antes de un | ó +)
- ✓ | Quita un prefijo de discado del número (Por ejemplo: 300|NXXXXXX equivaldrá cuando alguien marque 30035551234, pero sólo ingresará en la troncal 5551234)
- ✓ + Suma un prefijo de discado al número marcado (Por ejemplo: 300+NXXXXXX equivaldrá cuando alguien marca 5551234 e ingresará a la troncal como 3005551234)

2.1.7. EXTENSIONES RESERVADAS

Extensiones	Uso Reservado
200	Notificación de Parqueo
300 a 399	Marcación Rápida
666	Prueba de Fax
70 a 79	Llamada en Espera

700 a 799	Llamada en Espera
7777	Simulación de Llamada Entrante

3. ELASTIX

Elastix es un software aplicativo que integra las mejores herramientas disponibles para PBXs basados en Asterisk en una interfaz simple y fácil de usar. Además añade su propio conjunto de utilidades y permite la creación de módulos de terceros para hacer de este el mejor paquete de software disponible para la telefonía de código abierto.

La meta de Elastix son la confiabilidad, modularidad y fácil uso. Estas características añadidas a la robustez para reportar hacen de él la mejor opción para implementar un PBX basado en Asterisk.

4. TRIXBOX

Trixbox, conocido previamente con el nombre de Asterisk@Home, es una solución que permite instalar Asterisk y un paquete de programas vinculados a su administración y uso vía Web, los cuales son instalados conjuntamente desde un CD booteable.

5. RED VPN

5.1. NECESIDADES Y SURGIMIENTO DE LAS VPNS

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.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

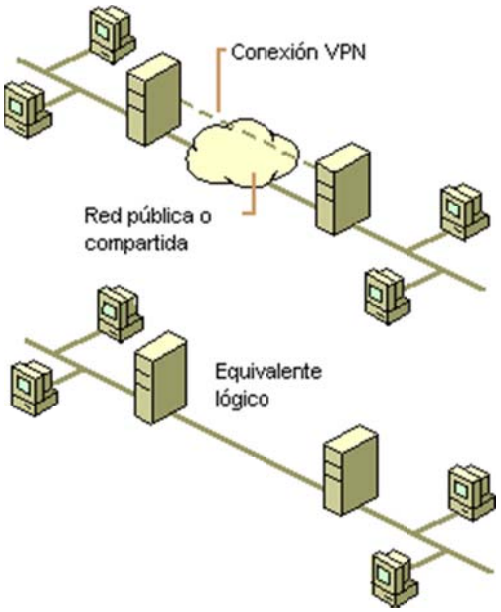
Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services (RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan.

Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

5.2. ESTRUCTURA DE LAS VPNS

Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura siguiente, la idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.



Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene

lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.

La tecnología de túneles (“Tunneling”) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los

datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Ejemplos de sistemas de autenticación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de la poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de proposals del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

5.3. PROTOCOLOS UTILIZADOS EN LAS VPNS

5.3.1. PPTP

Point-to-Point Tunneling Protocol fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego “llaman” al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

- el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

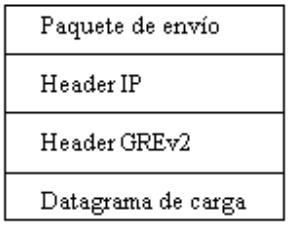


Figura 3 Capas del Encapsulamiento PPTP

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

5.3.2. IPSEC

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un Gateway:

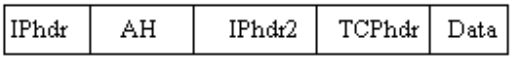
- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP

cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

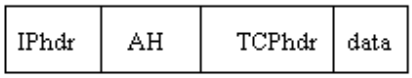
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un Gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del Gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

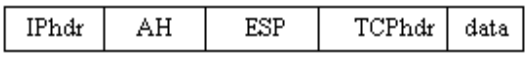
Un ejemplo de paquete AH en modo túnel es:



Un ejemplo de paquete AH en modo transporte es:

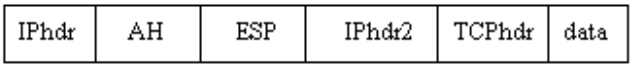


Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:



Este tipo de paquete se denomina Transport Adjacency.

La versión de entunelamiento sería:



Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

5.3.3. L2TP

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.
El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:

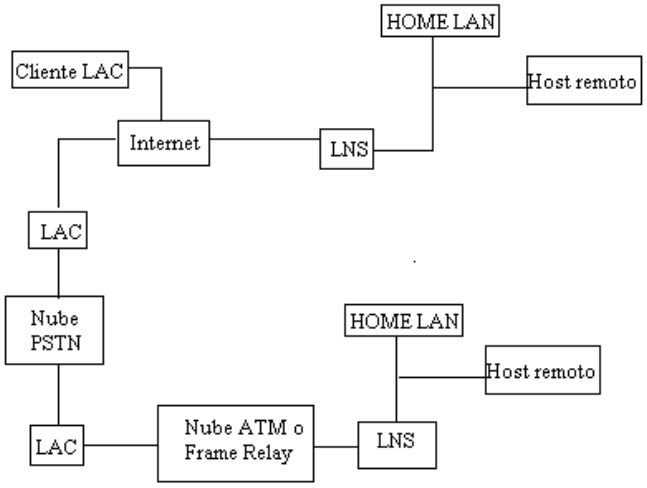


Figura 4 Marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío.

Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

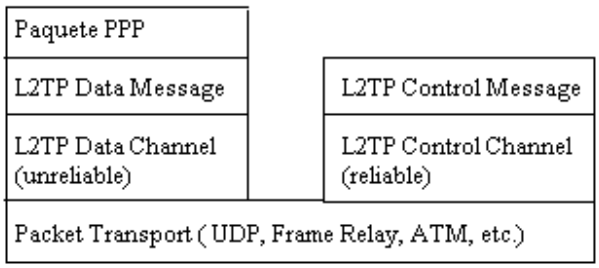


Figura 5 Relación entre los marcos PPP y los mensajes de control

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.
Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

5.4. CONFIGURACIÓN DE PROTOCOLOS

5.4.1. CONFIGURACIÓN DE UNA VPN BAJO WINDOWS

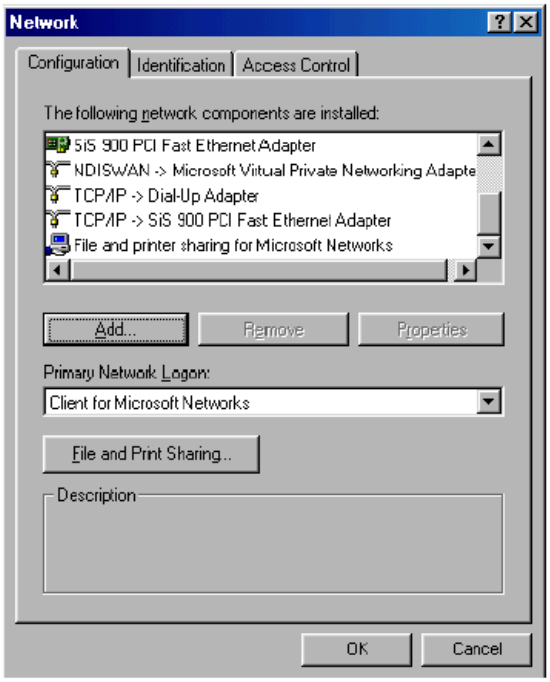
PARA CONFIGURAR UNA VPN BAJO WINDOWS SE NECESITA LO SIGUIENTE:

- Conexión a Internet tanto para el servidor local de NT como para las máquinas remotas.
- Una dirección IP estática para el servidor NT.
- Proxy que se ejecute en el servidor NT, para evitar el acceso desautorizado al sistema.
- Direcciones IP para los recursos a compartir.
- Adaptador virtual de la red instalado en la máquina remota o cliente.

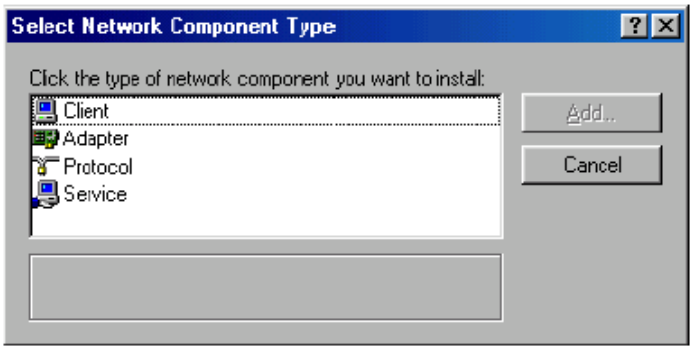
- La secuencia de pasos es:
    - Hacer una lista de las direcciones IP de los recursos que serán compartidos a través de Internet.
    - Instalación y ejecución del proxy.
    - En el servidor NT, se deben configurar los archivos del usuario NT para que pueda llamar y conectarse al servidor, garantizando su acceso al sistema con los permisos de la VPN.

Luego de estos pasos, se deberá instalar el adaptador privado de la red en la máquina cliente, como se indica:

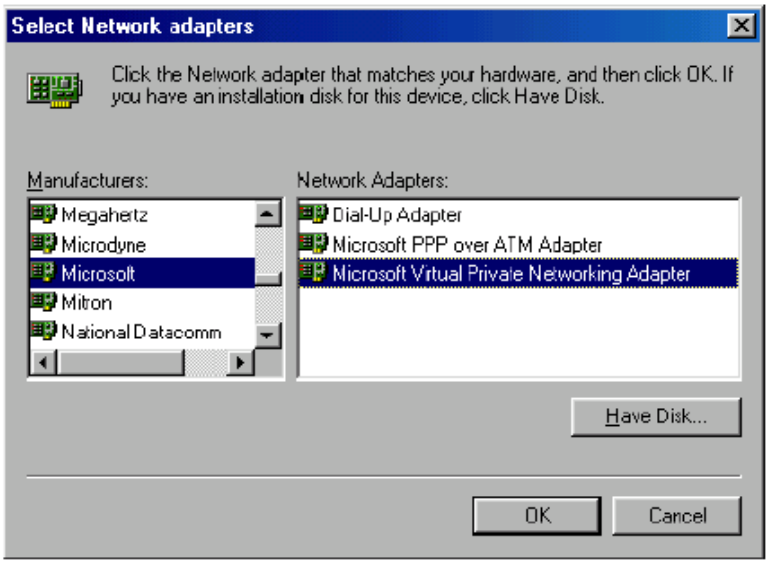
- Dentro del Diálogo de Red, que se muestra debajo, y al cual se accede a través de la opción Propiedades del icono Entorno de Red, se presiona el botón Add.



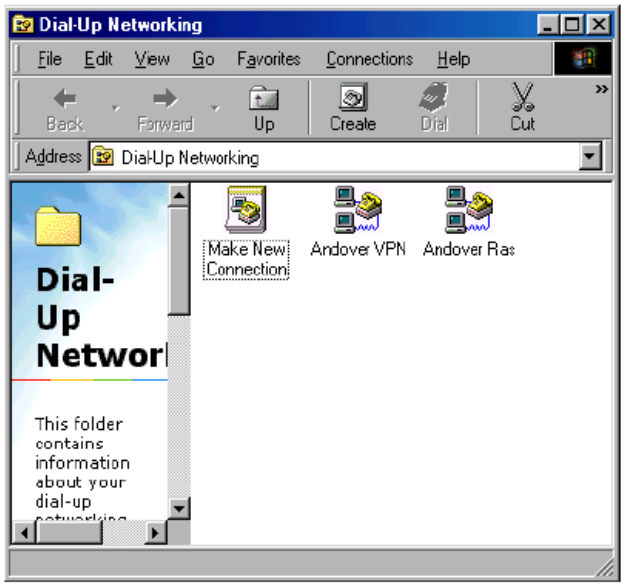
- Aparecerá la siguiente pantalla, se deberá seleccionar Adapter y luego presionar el botón Add.



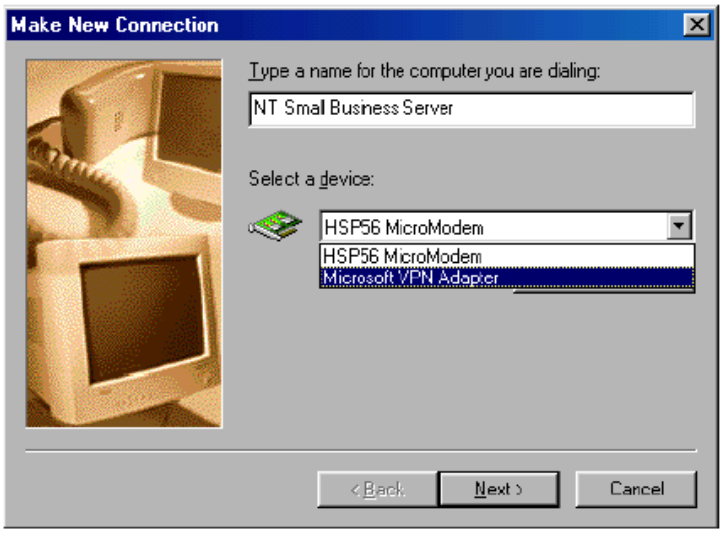
- Aparece el cuadro Select Network adapters, donde se deberá elegir el fabricante y el adaptador como se muestra en la siguiente figura:



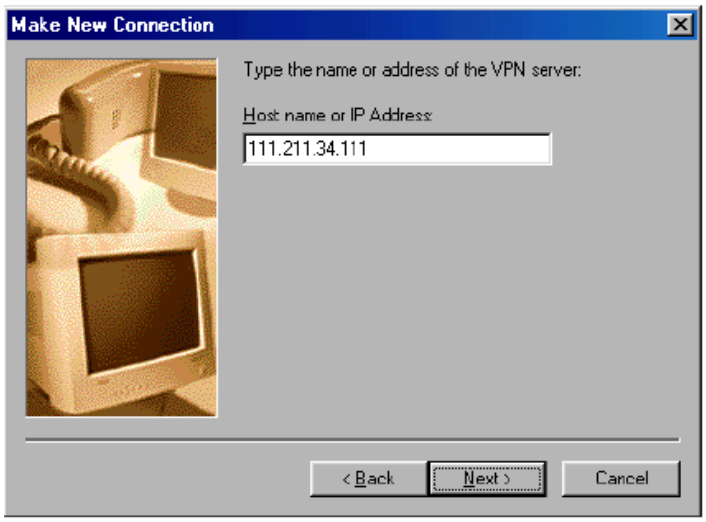
- Posteriormente, para instalar la conexión a la LAN, se deberá acceder al Acceso Remoto a Redes



- Se selecciona Make a New Connection, apareciendo la siguiente pantalla, donde se podrá elegir el adaptador de VPN:

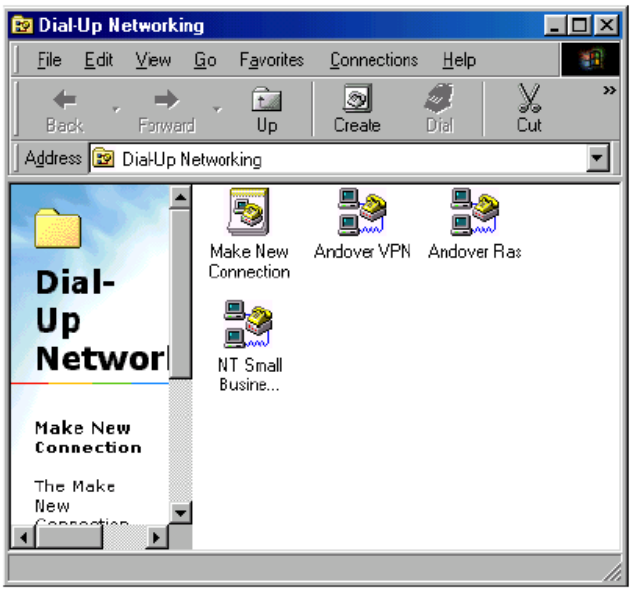


- Luego de presionar el botón Next, se deberá introducir la dirección IP del servidor VPN en la siguiente pantalla:

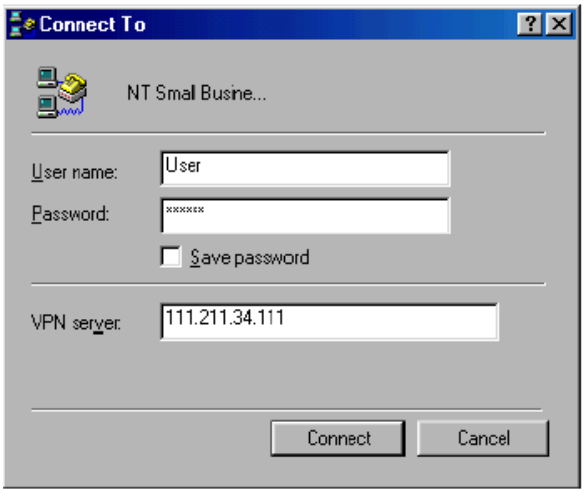


- Así se finaliza la creación de la nueva conexión:

Para acceder al servidor NT, se abre el Acceso Remoto a Redes:



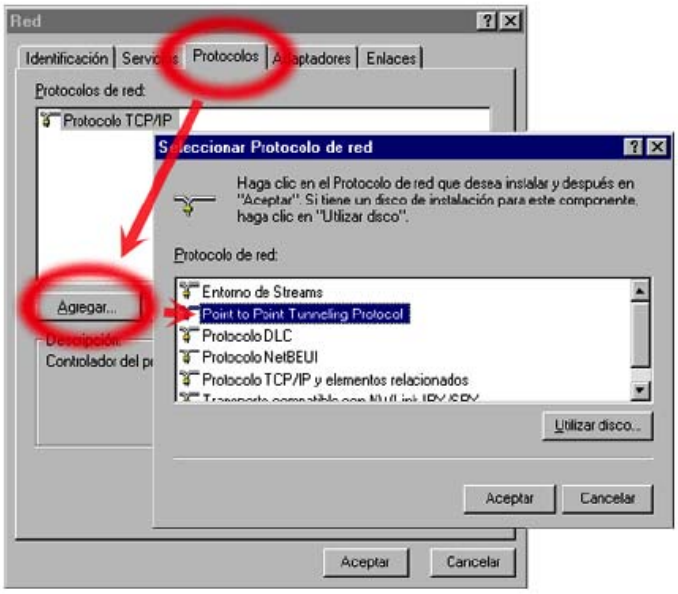
Al hacer doble-click en el icono de la conexión VPN, aparecerá la siguiente pantalla, donde se debe introducir el nombre de usuario, la contraseña y la dirección IP del servidor NT:



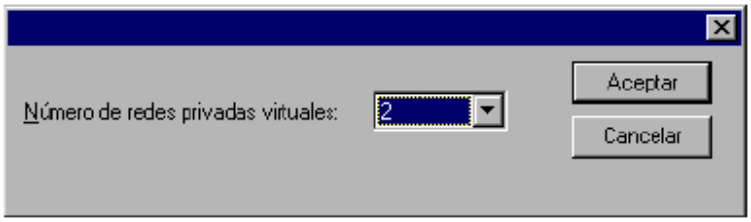
Para configurar el servidor VPN, se deberá configurar PPTP, activar el filtro PPTP y activar el soporte PPTP en los clientes.

Para configurar PPTP en el servidor RAS y en los clientes que vayan a utilizarlo, se deberán realizar los siguientes pasos:

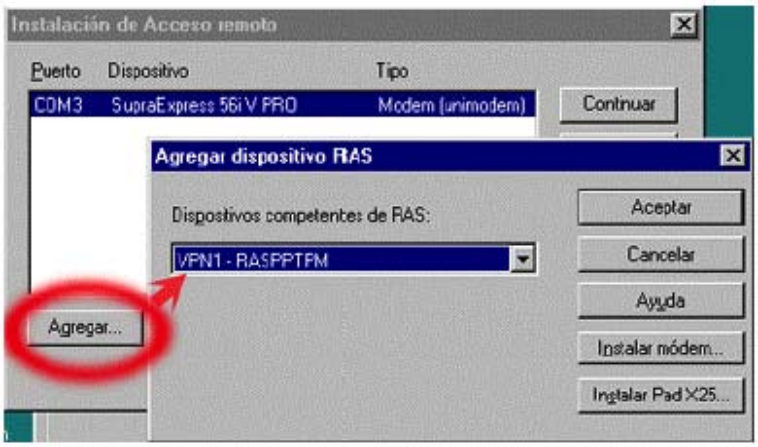
- Dentro de Red en el Panel de Control, seleccionando Protocolos, se deberá presionar el botón Agregar:



- Se selecciona Point to Point Tunneling Protocol, y, luego de copiados los archivos, aparecerá el cuadro de diálogo Configuración de PPTP. El campo Número de redes privadas virtuales indica el número de conexiones PPTP admitidas. En el ejemplo, se establecen 2 VPN:



- Luego, se inicia la herramienta de configuración RAS, donde se deben añadir los puertos virtuales que darán servicio a las redes privadas virtuales que se deseen establecer. Al presionar el botón Agregar, se accede al dialogo Agregar dispositivo RAS:



- Después de ingresadas las entradas, se presiona Aceptar. Luego se podrá seleccionar cada entrada del diálogo Instalación de Acceso Remoto, para configurar el uso del puerto. Las opciones son: Sólo recibir llamadas o Hacer y recibir llamadas.
- Después de añadir todos los dispositivos virtuales, se podrá cerrar este diálogo para volver a la ficha Protocolos. Al reiniciar la computadora, ya estará configurado el server.

Para la activación del filtro PPTP, se debe selecciona la solapa Protocolos de Panel de Configuración / Red. Dentro de esta pantalla, se elige Protocolo TCP/IP, luego Propiedades. En la solapa Dirección IP, se selecciona el adaptador de red sobre el que se aplicará el filtro. Luego de presionar el botón Avanzadas, se marca la casilla Activar filtro PPTP y, por último, se reinicia la máquina para activar la configuración.

Cuando un cliente se conecta a Internet, el procedimiento para establecer un túnel VPN consta de dos pasos:

- Establecimiento por parte del cliente mediante una conexión de acceso telefónico a través de un ISP.
- Establecimiento de una conexión PPTP con el servidor RAS.

Cuando un cliente se conecta directamente a Internet, no es necesario establecer una conexión de acceso telefónico. Sin embargo, el procedimiento para iniciar la conexión PPTP con el servidor RAS es idéntico. Para establecer una conexión PPTP es necesario crear una entrada especial en la guía telefónica. Esta entrada se distingue por dos características:

- El campo Marcar utilizado tiene uno de los dispositivos virtuales VPN añadidos a la configuración RAS al instalar PPTP. Esta lista sólo muestra los VPN configurados para hacer llamadas.
- El campo Presentación preliminar de número telefónico contiene el nombre DNS o la dirección IP del servidor PPTP.

La creación de una conexión PPTP implica también dos pasos:

- Se abre la aplicación Acceso telefónico a redes, utilizando la guía telefónica que permite acceder al ISP a través de un número de teléfono y un modem.
- Establecida la conexión, se debe abrir la entrada de la guía telefónica que se conecta al túnel PPTP mediante un nombre DNS o una dirección IP.
  Si el cliente está conectado directamente a Internet, sólo es necesario el segundo paso.

5.4.2. CONFIGURACIÓN DE UNA VPN BAJO LINUX

VPND permite crear enlaces seguros sobre TCP/IP con claves de hasta 512 bits y algoritmo de encriptación BLOWFISH, montando una interfaz virtual serie que proporciona la posibilidad de enrutamiento de IP entre redes. Los pasos a seguir son:

- Dar soporte SLIP en el Kernel LINUX, recompilándolo y probando que funcione.

- Instalación del paquete vnpd, que, en Debian, se puede hacer con '**apt-get install vpnd**'.
- Creación de una clave de sesión, utilizando '**vpnd –m /etc/vnpd/vpnd.key**', que debe ser pasada al otro extremo de la VPN mediante un medio seguro, ya que es la clave que ambos extremos de la VPN comparten.
- Configuración de los extremos de la VPN, siguiendo la estructura Cliente/Servidor. A continuación, se muestran el contenido de los archivos **vpnd.conf** de configuración para el servidor y el cliente.

Archivo **/etc/vpn/vpnd.conf** para el servidor:

```
mode server
# Direccion IP y puerto del servidor
server a.b.c.d 2001
# Direccion IP y puerto del cliente
client w.x.y.z 2001
# Direccion IP privada del servidor
local a.b.c.d
# Direccion IP privada del cliente
remote w.x.y.z
# Opciones generales
autoroute
Keepalive 10
noanswer 3
keyfile /etc/vnpd/vnpd.key
pidfile /var/run/vpnd.pid
keyttl 120
ramdomdev /dev/urandom
mtu 1600
```

Archivo **/etc/vpn/vpnd.conf** para el cliente:

```
mode client
# Direccion IP y puerto del servidor
client w.x.y.z 2001
# Direccion IP y puerto del cliente
server a.b.c.d 2001
# Direccion IP privada del servidor
local w.x.y.z
# Direccion IP privada del cliente
remote a.b.c.d
# Opciones generales
autoroute
Keepalive 10
noanswer 3
keyfile /etc/vnpd/vnpd.key
pidfile /var/run/vpnd.pid
keyttl 120
ramdomdev /dev/urandom
mtu 1600
```

Una vez creados estos archivos, se podrá levantar la VPN, iniciando los demonios con '**/etc/init.d/vpnd start**'. Para comprobar el correcto funcionamiento, se puede hacer *pings* a las direcciones privada y del otro extremo y verificar con '**ifconfig –a**' que exista una nueva interfaz como la siguiente:

```
sl0      Link encap: VJ Serial Line IP
Inet addr: 10.0.0.1 P-t-P: 10.0.0.2 Mask : 255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST
MTU: 1600
 Metric: 1
Rx packets: 0 errors: 0 dropped: 0 overruns: 0 frame: 0
```

Compressed: 0
Tx packets: 0 errors: 0 dropped: 0 overruns: 0 carrier: 0
Collisions: 0 compressed: 0 txqueuelen: 10
RX bytes: 0 (0.0 b) TX bytes; 0 (0.0 b)

6. MIKROTIK

Mikrotīkls Ltd., conocida internacionalmente como **MikroTik**, es una compañía Letona vendedora de equipo informático y de redes. Vende principalmente productos de comunicación inalámbrica como routerboards o routers, también conocidos por el software que lo controla llamado RouterOS. La compañía fue fundada en el 1995, aprovechando el emergente mercado de la tecnología inalámbrica. En 2007, la compañía tenía más de 70 empleados.

El principal producto de Mikrotik es el sistema operativo conocido como Mikrotik RouterOS basado en Linux. Permite a los usuarios convertir un ordenador personal PC en un router, lo que permite funciones como firewall, VPN Server y Cliente, Gestor de ancho de banda, QoS, punto de acceso inalámbrico y otras características comúnmente utilizado para el enrutamiento y la conexión de redes. Existe un software llamado Winbox que ofrece una sofisticada interfaz gráfica para el sistema operativo RouterOS. El software también permite conexiones a través de FTP y Telnet, SSH y acceso shell. También hay una API que permite crear aplicaciones personalizadas para la gestión y supervisión.

Características principales

• El Sistema Operativo es basado en el Kernel de Linux y es muy estable.
• Puede ejecutarse desde discos IDE o módulos de memoria flash.
• Diseño modular
• Módulos actualizables
• Interfaz grafica amigable

Características de ruteo

• Políticas de enrutamiento. Ruteo estático o dinámico.
• Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en el bridge.
• Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
• Cache: web-proxy, DNS.
• Gateway de HotSpot.
• Lenguaje interno de scripts

Características del RouterOS

Filtrado de paquetes por:

- Origen, IP de destino.
- Protocolos, puertos.
- Contenidos (seguimiento de conexiones P2P).
- Puede detectar ataques de denegación de servicio (DoS)
- Permite solamente cierto número de paquetes por periodo de tiempo.
- Calidad de servicio (QoS)

Interfaces del RouterOS

• Ethernet 10/100/1000 Mbit.
• Inalámbrica (Atheros, Prism, CISCO/Airones)
• Punto de acceso o modo estación/cliente, WDS.
• Síncronas: V35, E1, Frame Relay.
• Asíncronas: Onboard serial, 8-port PCI.
• ISDN
• xDSL
• Virtual LAN (VLAN)

Herramientas de manejo de red

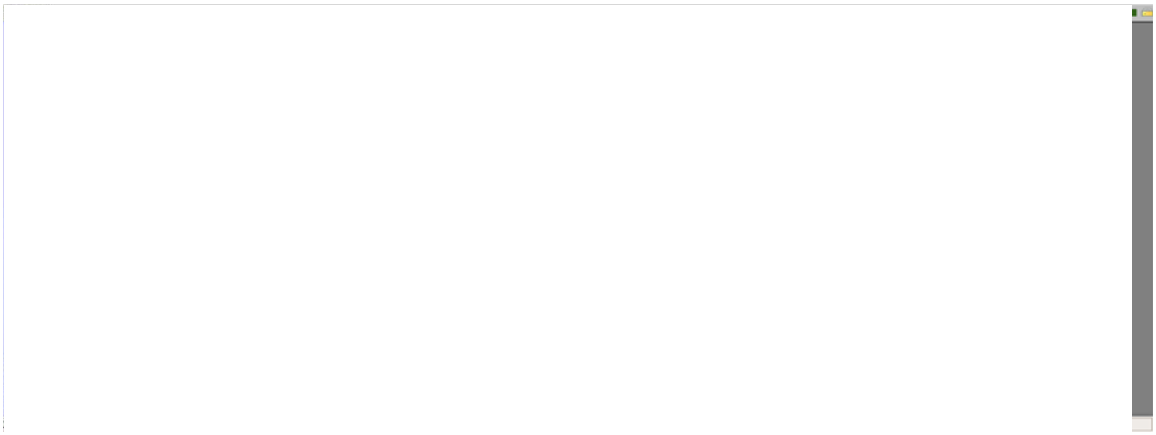
• Ping, traceroute.
• Medidor de ancho de banda.
• Contabilización de tráfico.
• SNMP.
• Torch.
• Sniffer de paquetes.

7. PROCEDIMIENTO PARA EFECTUAR VPN CON MIKROTIK

Se selecciona la opción del mikrotik para efectuar Vpn entre los clientes y la red interna corporativa de la siguiente manera:

Se escoge la opción PPP y se observa que existe una herramienta OVPN Server el cual se utiliza para configurar los clientes de Asterisk denominados remotos

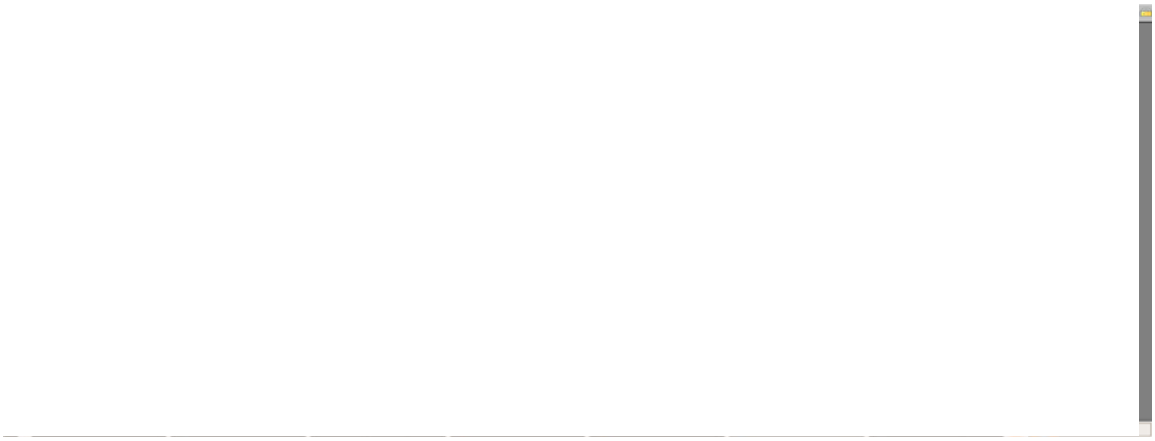
Se va a la opción PPTP Server y se habilita el OpenVpn Server

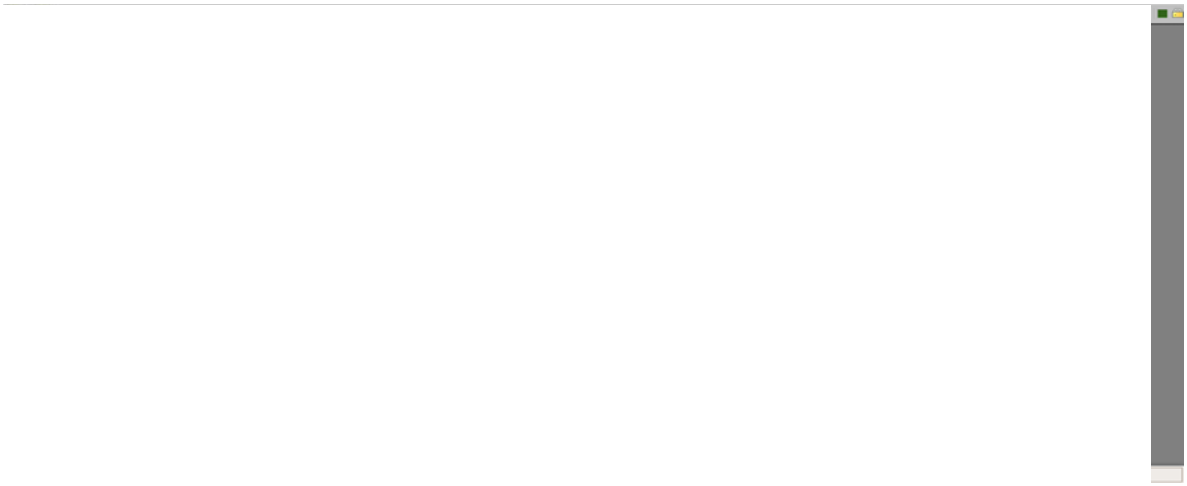


Los dos tipos de autenticación encriptados mschap1 y mschap2

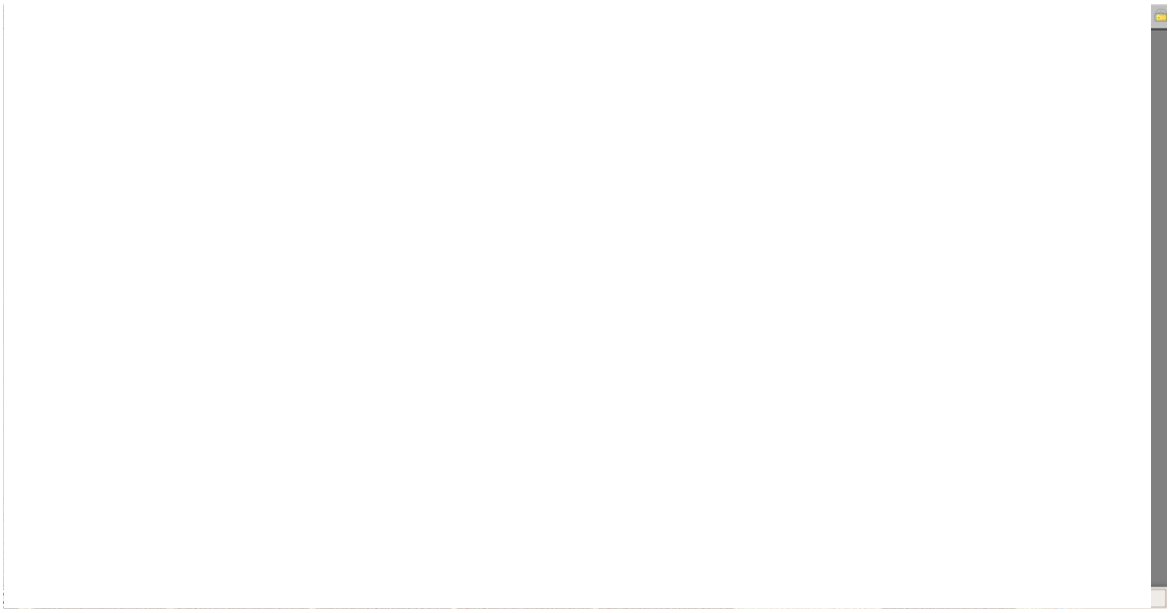
Ahora se escoge la opción de Profiles y se define el perfil de conexión para la red local para este caso llamado Asterisk

Se define las dos direcciones que son la local y la remota, la local pertenece al rango de red local WAN y la remota es la dirección que es asignada a la LAN de la VPN





Ahora en el Tab Secrets se ingresa el usuario “” para que se logee en la VPN del Asterisk con el password qwerty



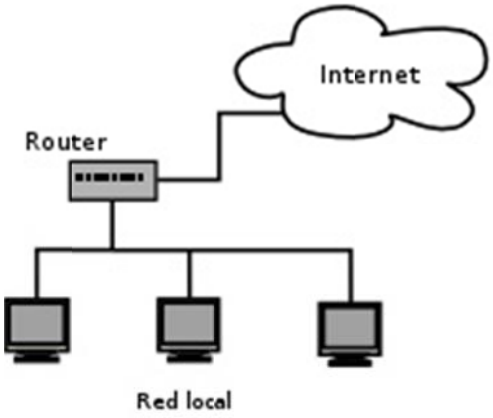
8. SOFTPHONE

Es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales usando un Proveedor de Servicios de VoIP. Un Softphone es típicamente parte de un entorno Voz sobre IP/VoIP y puede estar basado en el estándar SIP/IAX2/H.323 o ser propietario. Hay muchas implementaciones disponibles como el Sjphone, Xlite, etc.

9. NAT: Traducción de Direcciones de Red

La idea básica que hay detrás de NAT es traducir las IP´s privadas de la red en una IP pública para que la red pueda enviar paquetes al exterior; y traducir luego esa IP pública, de nuevo a la IP privada del PC que envió el paquete, para que pueda recibirlo una vez llega la respuesta. Con un ejemplo lo veremos mejor:

Imaginemos que tenemos nuestra siguiente red:



Podría ser la típica red casera en la que tenemos un par de PCs que salen a Internet a través del router. Cada PC tiene asignada una IP privada, y el router tiene su IP privada (puerta de enlace) y su IP pública (que es nuestra IP de Internet).

Cuando uno de los PCs de la red local quiere enviar un paquete a Internet, se lo envía al router (o a la puerta de enlace o gateway), y éste hace lo que se conoce como SNAT (Source-NAT) y cambia la dirección de origen por su IP pública. Así, el host remoto sabrá a qué IP pública ha de enviar sus paquetes. Cuando una respuesta o un paquete pertenecientes a esa conexión lleguen al router, éste traducirá la dirección IP de destino del paquete (que ahora es la IP del router) y la

cambiará por la dirección privada del host que corresponde, para hacer la entrega del paquete a la red local.

9.1. DNAT: Destinantion-NAT

Cuando iniciábamos una conexión desde la red local, se crea automáticamente una entrada en la tabla de NAT para que todo lo que perteneciera a esa conexión fuera dirigido hacia el PC correspondiente.
Pero si la conexión se inicia desde fuera ¿cómo y cuando se crea esa entrada en la tabla de NAT? La respuesta es que si queremos permitir conexiones desde el exterior a un PC de nuestra red local, hemos de añadir una entrada fija en la tabla de NAT, indicando que todo el tráfico que llegue que vaya a determinado puerto, sea dirigido al PC en cuestión.

El puerto es el único elemento que tenemos para “distinguir” conexiones, ya que todo llegará a la IP del router, pero tendrán un puerto de destino según sea una conexión u otra. Así que, en nuestro ejemplo, deberíamos crear una entrada fija en la tabla de NAT en la que indicáramos que lo que llegue al puerto 80 (web) sea dirigido al PC en el que corre el servidor web.

Esto es lo que se conoce habitualmente como “abrir puertos” en el router. Al abrir puertos, simplemente estamos añadiendo una entrada a la tabla de NAT.

Ya que desde el exterior, aunque nuestra red tenga varios PCs, se verá como si sólo fuera uno (solo se conoce la IP del router, éste lo traduce todo) y necesitamos que éste router al que le llega todo el tráfico sepa a quién ha de entregárselo.

9.2. FIREWALL

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como puede ser de la web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no de IRC que puede ser innecesario para nuestro trabajo.

También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes.

Para la ejecución del proyecto se utilizo una Computadora a la que se le instalo el software de acceso libre llamado MONOWALL (es un software que usado junto con una PC embebida ofrece todas las características más importantes disponibles en las alternativas de hardware de firewall comercial.) permitiendo manejar las funciones de VPN, NAT y de protección de puertos para la telefonía.

9.2.1. MONOWALL

Monowall no es un enrutador. Es más bien un muro de seguridad que puede ser configurado para diversos escenarios incluyendo Nat 1:1, lo cual le permite administrar IPs publicas dentro de la red interna. Dentro de las funciones más destacables de Monowall se encuentran:

- Interfaz de consola serial
- Interfaz Web
- Soporte para redes inalámbricas
- Portal cautivo
- Soporte para Redes virtuales
- Filtrado de Paquetes
- NAT/PAT
- DHCP
- VPNs
- Acelerador DNS
- Agente de transferencia SMTP
- Moldeado de Trafico

CAPITULO 2

10. UNIRED

Es una corporación mixta, sin ánimo de lucro, que tiene como objeto, operar, directa o indirectamente, redes telemáticas y servicios relacionados con éstas, y desarrollar estrategias para la consolidación de una cultura de sistemas de información y de redes en la sociedad colombiana con el fin de dar un mejor aprovechamiento de los recursos con que cuentan sus asociados en el desarrollo integral de servicios y el fortalecimiento del sector educativo de la región.

Los servicios principales que ofrece UNIRED son:

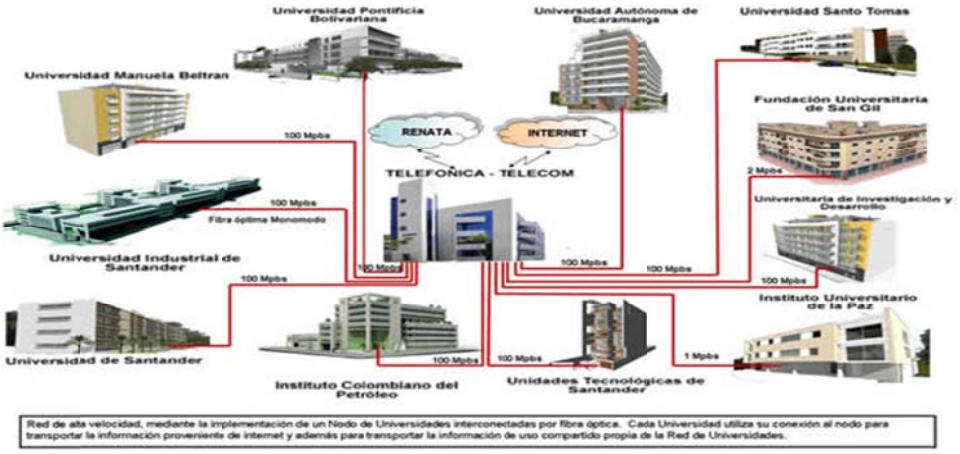
- Compartir material bibliográfico y digital.
- Aprovechar el material intelectual producido en las universidades por profesores y alumnos.
- Conectar las universidades a internet a través de fibra óptica a la red nacional.
- Adquirir servicios de internet, software y hardware entre las universidades.

10.1. MIEMBROS DE UNIRED

- Universidad Industrial de Santander
- Universidad Autónoma de Bucaramanga
- Universidad Santo Tomás
- Universidad Pontificia de Bucaramanga
- Instituto Colombiano del Petróleo
- Corporación Universitaria de Investigación y Desarrollo UDI.
- Universidad Cooperativa de Colombia
- Universidad de Santander
- Instituto Universitario de la Paz UNIPAZ

- Unidades Tecnológicas de Santander
- Fundación Universitaria de San Gil
- ADEL METROPOLITANA
- Universidad Manuela Beltrán
- Universidad de Boyacá
- Universidad Pedagógica y Tecnológica de Colombia

10.2. CONECTIVIDAD



UNIRED maneja un dispositivo Switch multicapa de Cisco que permite trabajar con calidad de servicio (QoS).

11. RENATA

La Red Nacional Académica de Tecnología Avanzada (RENATA) es la red colombiana de nueva generación que conecta a las universidades y los centros de investigación del país entre sí, y a estos, a través de la Red CLARA, con las redes internacionales de alta velocidad y los centros de investigación más desarrollados del mundo.

RENATA es una iniciativa de las redes regionales Colombianas actualmente en funcionamiento, tales como RUANA, RUAV, RUMBA, RUMBO, RUP y UNIRED, a las cuales están vinculadas las principales instituciones de educación superior y centros de investigación de las diferentes regiones del país.

11.1. MIEMBROS DE RENATA

RUANA: UNIVERSIDADES MEDELLÍN

Universidad de Antioquia
EAFIT
CES
Escuela de Ingeniería de Antioquia
Corporación Universitaria Lasallista
Universidad Nacional
Universidad Pontificia Bolivariana
Universidad de Medellín

RUAV: UNIVERSIDADES CALI

Universidad del Valle
Universidad Javeriana
ICESI
Universidad Autónoma de Occidente
Universidad San Buenaventura

Universidad Santiago de Cali
Universidad Libre
Centro Internacional de Agricultura Tropical (CIAT)

RUMBO: UNIVERSIDADES BOGOTÁ

Escuela de Administración de Negocios
Escuela Colombiana de Ingeniería
Politécnico Grancolombiano
Pontificia Universidad Javeriana
Universidad Católica de Colombia
Universidad Jorge Tadeo Lozano
Universidad de la Sabana
Universidad de los Andes
Universidad del Rosario
Universidad Nacional de Colombia

RUMBA: UNIVERSIDADES BARRANQUILLA

Corporación Universitaria de la Costa
Universidad Libre de Barranquilla
Universidad Metropolitana
Corp. Educ. Mayor del Desarrollo Simón Bolívar
Universidad Autónoma del Caribe
Universidad del Norte

UNIRED: UNIVERSIDADES BUCARAMANGA

Universidad Industrial de Santander
Universidad Autónoma de Bucaramanga
Universidad Pontificia Bolivariana
Universidad Santo Tomás
Universitaria de Investigación y Desarrollo
Instituto Colombiano del Petróleo

Universidad de Santander.
Instituto Universitario de la Paz UNIPAZ.
Unidades Tecnológicas de Santander.
Fundación Universitaria de San Gil.
Universidad Manuela Beltrán

RUP: UNIVERSIDADES POPAYÁN

Universidad del Cauca
Universidad Cooperativa de Colombia
Fundación Universitaria Popayán
Colegio Mayor del Cauca
Instituto Tecnológico de Comfacauca
SENA Regional Cauca
Corporación Universitaria Autónoma

11.2. CONECTIVIDAD

RENATA transita sobre un ancho de banda de 200 Mbps. La infraestructura de la Red Nacional Académica de Tecnología Avanzada, RENATA, está basada en una topología de estrella jerárquica donde el punto central es la sede Morato de Colombia Telecomunicaciones en Bogotá, los puntos de la estrella los conforman los nodos principales de las Redes Académicas Regionales de las ciudades de Cali, Barranquilla, Medellín, Bucaramanga, Pereira (Eje Cafetero), Popayán y Bogotá, en donde se interconectan a cada uno de los operadores locales que manejan las redes metropolitanas de las universidades.

La transmisión se realiza por la red MPLS de Colombia Telecomunicaciones a nivel de E1´s con un tiempo de convergencia de la red MPLS del anillo nacional de fibra óptica de 50 ms de acuerdo con el modelo planteado.

Entre los mecanismos de acceso soportados se cuenta con servicios para interfaces “Ethernet 10/100/1000” tanto en los multiplexores como en los

enrutadores. Igualmente, los puertos sobre los servicios soportan transporte transparente (“Port Mode”) o a través de VLANs (cubre “Stacked VLANs”) para conexiones virtuales a través de un mismo puerto. Los nodos de acceso con interfaces “10/100BASET” son los encargados de recibir los enlaces de los operadores locales de cada red regional.

Cada nodo de la red se interconecta a través de una interfaz “GigaEthernet” o “FastEthernet” de acuerdo con la topología de cada operador local. Cada nodo de acceso maneja 200Mbps hacia el nodo de concentración en Morato-Bogotá garantizando los tiempos de convergencia de 40 ms en caso de falla de la red MPLS.

La capacidad actual de cada uno de los enlaces a nivel nacional es de 200 Mbps en MPLS. Esta capacidad es entregada por la red MPLS de Colombia Telecomunicaciones a nivel de 5*E1´s en cada uno de los nodos de las diferentes redes como Barranquilla, Bucaramanga, Cali, Popayán, Medellín, Eje cafetero y Bogotá.

La red MPLS entrega su capacidad en E1´s a un equipo multiplexor Metro 500 a nivel nacional, Metro 1000 en Bogotá en interface G703, el equipo multiplexor agrupa los E1´s y los entrega en interface Ethernet al equipo enrutador Cisco 7606 conformando así la red nacional. Los operadores entregan en interface Ethernet a un puerto “FastEthernet” del Cisco 7206, en el caso Bogotá la interconexión se realiza directamente al puerto “FastEthernet” del equipo a nivel de 802.1q.


Baq
Buc
Mde
Bog
Cio
Pyy
RENATA

CAPITULO 3

12. ACTIVIDADES

A continuación se describirán las actividades realizadas antes de la Instalación Básica piloto entre los puntos mencionados en el ítem numero 11.

Actividad No 1	Fecha	Objetivo	Observación
Se precedió a instalar la versión para Windows del software VMware*Station Versión 6.0.4 y se hicieron pruebas de funcionalidad y compatibilidad.	02- 5 - 2010	Explorar funcionalidad y compatibilidad	Bien

Tabla 1. Actividad No 1

Actividad No 2	Fecha	Objetivo	Observación
Después sobre el software VMware se instalo el sistema operativo Debian de Linux con Kernel 2.6 y se realizaron pruebas de funcionalidad y concurrencia.	02- 10 - 2010	Verificar funcionalidad y concurrencia	Bien

Tabla 2. Actividad No 2

Actividad No 3	Fecha	Objetivo	Observación
Se precedió a instalar sobre el sistema operativo	02- 15 – 2010	Comprobar funcionalidad,	Bien

Debian el software de código libre Asterisk en la versión 1.4 y se realizaron pruebas de funcionalidad, compatibilidad y rendimiento.		compatibilidad y rendimiento	

Tabla 3. Actividad No 3

Actividad No 4	Fecha	Objetivo	Observación
Se instalo la versión para Windows del SoftPhone X-LITE con su respectiva diadema y se hicieron pruebas de comunicación con el servidor para averiguar funcionalidad.	02- 20 - 2010	Explorar funcionalidad	Bien

Tabla 4. Actividad No 4

Actividad No 5	Fecha	Objetivo	Observación
Después de haber realizado las pruebas con el SoftPhone X-LITE y el servidor Asterisk se continúo revisando otras funciones, como el buzón de mensajes y la calidad del sonido.	02- 25 - 2010	Verificación del buzón de mensajes y la calidad del sonido	Bien

Tabla 5. Actividad No 5

Actividad No 6	Fecha	Objetivo	Observación
Las pruebas realizadas anteriormente fueron exitosas, ya que el servidor contaba con los requerimientos necesarios, gracias a ello se empezó a realizar pruebas con dos usuarios Windows en computadores diferentes.	02- 30 - 2010	Verificación funcionalidad entre dos usuarios Windows.	Bien

Tabla 6. Actividad No 6

Actividad No 7	Fecha	Objetivo	Observación
Después de realizadas las pruebas con los dos usuarios se procedió a ejecutar los procesos y las pruebas correspondientes para la conexión entre dos servidores Asterisk.	02- 01 - 2010	Verificación de funcionalidad y conexión entre dos servidores Asterisk.	Bien

Tabla 7. Actividad No 7

Actividad No 8	Fecha	Objetivo	Observación
El siguiente paso fue realizar las pruebas de funcionalidad y conexión entre dos usuarios de diferente servidor Asterisk	02- 10 - 2010	Verificación de funcionalidad y conexión entre dos usuarios de servidores Asterisk diferentes.	Bien

dentro del mismo punto de trabajo.			

Tabla 8. Actividad No 8

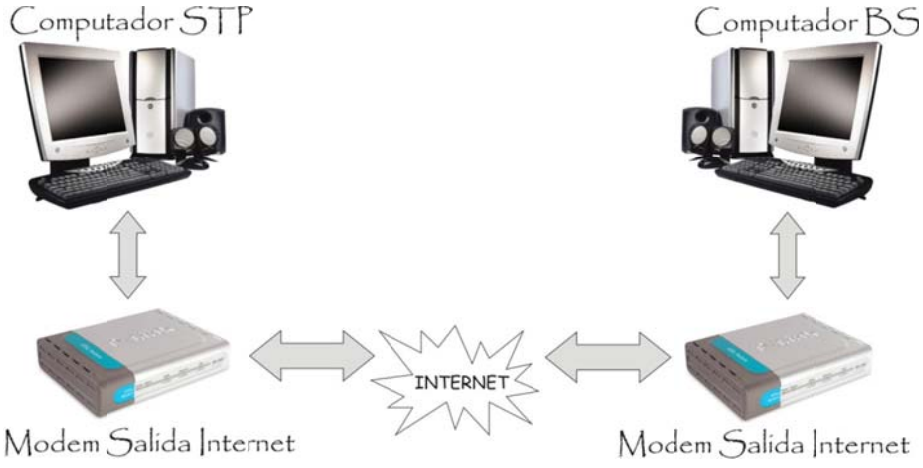
Actividad No 9	Fecha	Objetivo	Observación
Por último se procedió a trasladar uno de los servidores Asterisk fuera del punto de trabajo y de la red para hacer pruebas de conectividad y funcionalidad.	02- 20 - 2010	Verificación de funcionalidad y conectividad con los servidores Asterisk en diferentes redes.	Bien

Tabla 9. Actividad No 9

13. INSTALCIÓN BASICA PILOTO ENTRE LA EMPRESA BUSINESS STRATEGY LTDA DE GIRÓN Y LA SEDE DE TRABAJO DEL PROYECTO EN LA CIUDAD DE BUCARAMANGA.

Se procederá a explicar los pasos para la instalación de las centralitas IPBX que permitirá hacer la conexión entre la EMPRESA BUSINESS STRATEGY LTDA y LA SEDE DE TRABAJO DEL PROYECTO.

Las centralitas se montaran con el software de código libre Asterisk en la versión 1.4 sobre el sistema operativo Debian de Linux con Kernel 2.6, siendo el sistema operativo de mejor resultado. Hay que tener cuidado cuando se instala Asterisk ya que borra totalmente los archivos y sistema operativo que tengas en tu computador por ello se utilizara para nuestra conexión el software VMware*Station Versión 6.0.4 que permite instalar sobre el computador un nuevo sistema operativo sin afectar el sistema operativo con que trabaja.
Los Computadores que servirán para la instalación de las centralitas poseen los siguientes componentes y capacidades:



Computador (Sede de Trabajo del Proyecto)	Computador (Empresa BS Ltda.)
▪ Procesador de 2 GHz	* Procesador de 2 GHz
▪ Memoria RAM de 1 GHz	* Memoria RAM 1 GHz
▪ Disco Duro de 160 GHz	* Disco Duro de 160 GHz
▪ Tarjeta de red 10/100	* Tarjeta de red 10/100

13.1. PAQUETES REQUERIDOS PARA LA INSTALACIÓN DE LAS CENTRALITAS ASTERISK

A medida que Asterisk ha ido avanzando con el tiempo se han visto cambios en los paquetes que requiere, para el caso del enlace es indispensable tener los siguientes paquetes:

- ✓ Libpri-1.4: Este paquete es necesario cuando pensamos usar interfaces T1 o E1.
- ✓ Dahdi-1.4: requerido si vamos a usar hardware Digium o requerimos instalar ztdummy que es esencial para ejecutar algunas aplicaciones (meetme).
- ✓ Asterisk-1.4: Es una aplicación de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX).

- ✓ Asterisk-addons-1.4: Es un paquete que permite integrar a nuestra central de telefonía ip, tres funcionalidades muy importantes como son:

- ➢ Tener un registro de las llamadas en un data base usando MySql (si deseamos con base de datos)
- ➢ Poder utilizar archivos MP3 para la música en espera

- Añadir el protocolo H.323 fue diseñado con un objetivo principal: Proveer a los usuarios con tele-conferencias que tienen capacidades de voz, video y datos sobre redes de conmutación de paquetes.

- ✓ Bison: Este es necesario para compilar el Asterisk.

- ✓ Ncurses y ncursesdevelopment: Son requeridos si se desean construir nuevas herramientas (ej. Astman).

- ✓ Zlib y zlibdevel: son necesarias ahora para compilar, esto debido a la adhesión del protocolo DUNDI (Distributed Universal Number Discovery).

13.2. INSTALACION DE LOS PAQUETES DE ASTERISK REQUERIDOS

Requisitos: maquina Asterisk con salida a Internet

Los paquetes requeridos serán instalados en el directorio /usr/src del sistema operativo Debian, los paquetes son:

1. Lipri-1.4 (current)
2. Dahdi-1.4
3. Asterisk-1.4
4. Asterisk-addons-1.4

Para el funcionamiento correcto de nuestros paquetes se debe descargar librerías y compiladores. Para ello debemos editar con la función nano el siguiente directorio /etc/apt/sources.list y agregarle las direcciones de internet donde se encuentran, de esta forma:

deb http://ftp.debian.org/debian etch main contrib

deb http://mirrors.kernel.org/debian etch main contrib

A continuación ejecutamos el siguiente comando “aptitude update” para descargar de las páginas las librerías y compiladores.

Después ejecutamos el siguiente comando uname –r (se utiliza para mostrar información sobre el sistema) que nos arroja el resultado del kernel que es 2.6.18-6-486 este valor se cambia por ‘uname-r’ del siguiente comando “apt-get install Linux-headers- ‘uname-r’ (nos sirve para actualizar el kernel)” y se ejecuta.

Ahora debemos instalar las dependencias:

apt-get install libncurses-dev make automake autoconf gcc g++ bison libncurses5-dev libssl-dev libnewt-dev zlib1g-dev initrd-tools cvs procps curl libcurl3-dev mpg123 libmysql++-dev mysql-client pciutils openssl libasound2-dev libc6-dev zlib-bin

A continuación bajaremos los paquetes requeridos para la instalación de Asterisk de la siguiente manera:

- wget http://downloads.digium.com/pub/libpri/libpri-1.2-current.tar.gz
- wget http://downloads.digium.com/pub/telephony/dahdi-linux-complete current.tar.gz
- wget http://downloads.digium.com/pub/asterisk/asterisk-1.4-current.tar.gz
- wget http://downloads.digium.com/pub/asterisk/asterisk-addons-1.4-current.tar.gz

Después serán ubicados en el directorio /usr/scr del sistema operático Debian, desde allí empezaremos a descomprimir los paquetes como veremos a continuación:

- tar –zxvf lipri-1.4-current.tar.gz
- tar –zxvf dahdi-lunux-complete-current.tar.gz
- tar –zxvf asterisk-1.4-current.tar.gz
- tar –zxvf asterisk-addons-1.4-current.tar.gz

Luego de tenerlos descomprimidos empezaremos a instalarlos así:

Para LIBPRI

- Asterisk1:/# cd /usr/src
- Asterisk1:/usr/src# cd libpri-1.4.9
- Asterisk1:/usr/src/libpri-1.4#
    - make
    - make install

➢ **Para DAHDI**

- Asterisk1:/# cd /usr/src
- Asterisk1:/usr/src# cd dahdi-1.4
- Asterisk1:/usr/src/dahdi-1.4#
    - make clean
    - make
    - make install

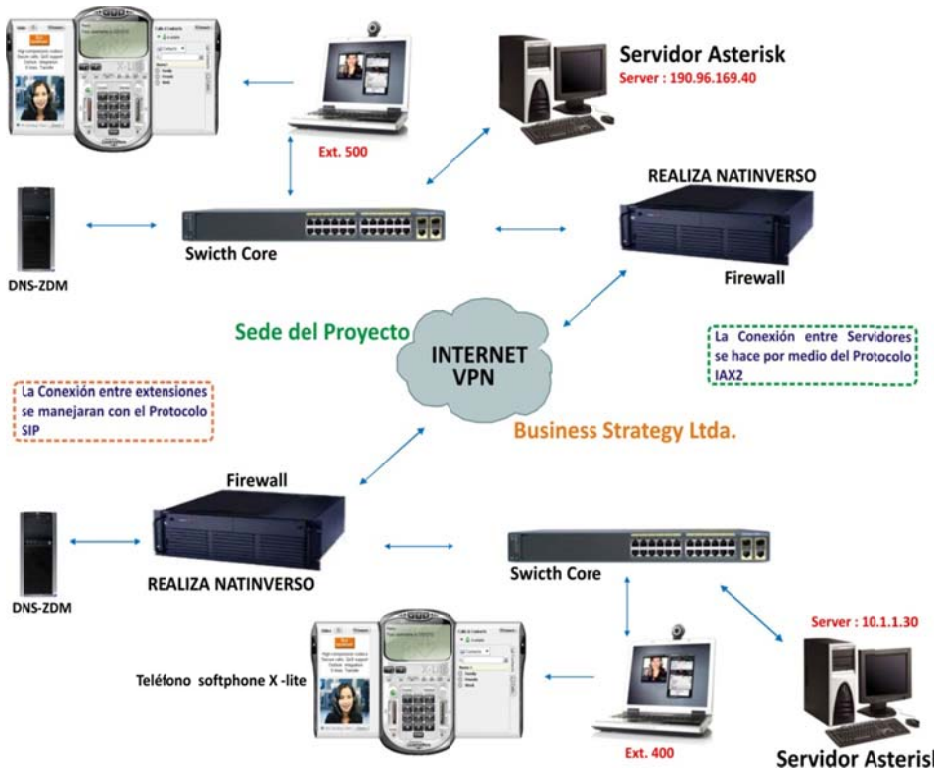
➢ **Para ASTERISK**

- Asterisk1:/# cd /usr/src
- Asterisk1:/usr/src# cd asterisk-1.4
- Asterisk1:/usr/src/asterisk-1.4-1.4#
    - make clean
    - ./configure
    - make menuselect (Para visualizar el menú de instalación de Asterisk)
    - make

- ❖ make install
- ❖ make config (agregara los scripts de arranque en /etc/init.d/asterisk e iniciara el servicio Asterisk al encender la maquina)
- ❖ make samples (Archivos de configuración básica para poder arrancar el Asterisk)

Ahora aplicaremos el siguiente comando para instalar doxygen (herramienta para generación de documentación) con el siguiente comando apt-get install doxygen y después make progdocs (relacionado con doxygen).

13.3. ESQUEMA DE PRUEBAS DE CONEXIÓN ENTRE LA EMPRESA BUSINESS STRATEGY LTDA Y LA SEDE DE TRABAJO DEL PROYECTO.



Proyecto

Como se observa en la figura 11 se realizan la conexión vía telefonía IP que permite la comunicación de forma gratuita entre las sedes obteniendo el intercambio de información académica e investigativa utilizando un dispositivo llamado firewall que permite hacer NATINVERSO, esto con el fin de poder redirigir los puertos que son utilizados por los protocolos IAX2 (4569) y SIP (5060) para sus enlaces.

El protocolo IAX2 se utiliza para las diferentes conexiones de las sedes y el protocolo SIP se usa entre las diferentes Extensiones internas que se requieran en las sedes. También se observa que la conexión se hace más segura por medio de una VPN ya que los paquetes viajan a través de infraestructuras públicas (Internet) en forma encriptada y a través del túnel de manera que es prácticamente ilegible para quien intercepte estos paquetes.

13.4. CREACION DE EXTENSION TIPO SIP PARA LA COMUNICACION ENTRE LAS SECRETARIAS DE LA EMPRESA BUSINESS STRATEGY LTDA. Y LA SEDE DE TRABAJO DEL PROYECTO

Se crea la extensión SIP de la Empresa con el número 400 de la siguiente forma:

Editamos el archivo sip.conf que nos permite crear la extensión IP agregándole los siguientes parámetros:

```
[general]
bindport = 5060
bindaddr = 10.1.1.30
context = default
disallow = all
allow = gsm
```

```
[400]
username = 400
type = friend
secret = 0000
host = dynamic
context = default
```

allow = alaw
allow = ulaw
nat = yes
language = es
maxexpirey = 120
defaultexpirey = 80
callerid = Bs <400>
qualify = yes

Se crea la extensión SIP de La Sede de Trabajo con el número 500 de la siguiente forma:

Editamos el archivo sip.conf que nos permite crear la extensión IP agregándole los siguientes parámetros:

[general]
bindport = 5060
bindaddr = 190.96.169.40
context = default
disallow = all
allow = gsm
allow = alaw
allow = ulaw
nat = yes
language = es
maxexpirey = 120
defaultexpirey = 80
[500]
username = 500
type = friend
secret = 0001
host = dynamic
context = default
callerid = Sp <500>
qualify = yes

13.5. DESARROLLO DEL PLAN DE DISCADO PARA NUESTRAS EXTENSIONES.

El dialplan (PLAN DE DISCADO) es el centro de operaciones del Asterisk, allí se define todo el proceso que realizara una llamada a través de unas instrucciones que son lanzadas a partir de dígitos recibidos a través de un canal o aplicación. El dialplan es la parte esencial de Asterisk sin este no puede funcionar.

En gran parte y la mayoría de modificaciones se realizaran en el archivo extensions.conf ubicado en /etc/asterisk/extensions.conf para editarlo lo abrimos usando nano desde consola:
Asterisk:~# nano /etc/asterisk/extensions.conf

Para el usuario de la Empresa haremos lo siguiente:

```
[general]

[global]

[default]
Include = conexion
Include = Buzon
Include = Ruta

[conexion]
exten = _4XX,1,Dial(SIP/${EXTEN},20)
exten = _4XX,2,Voicemail(${EXTEN})
```

Para el usuario de la Sede de Trabajo se hace lo siguiente:

[general]

[global]

[default]
Include = conexion
Include = Buzon
Include = Ruta

[conexion]
exten = _5XX,1,Dial(SIP/${EXTEN},20)
exten = _5XX,2,Voicemail(${EXTEN})

Creamos el Buzón para el usuario de la Empresa así:

[Buzon]
exten = _111,1,Voicemailmain(${CALLERID(num)})

Creamos el casillero editando el archivo voicemail.conf para el usuario de la Empresa así:

[default]
400 => 0000, Bs

Creamos el Buzón para el usuario de la Sede de Trabajo así:

[Buzon]
exten = _111,1Voicemailmain(${CALLERID(num)})

Creamos el casillero editando el archivo voicemail.conf para el usuario de la Sede así:

[default]
500 => 0001, Sp

Creamos la Ruta para el usuario de la Empresa así:

[Ruta]
exten = _8XXX,1,Dial(IAX2/servidor A/${EXTEN : 1},30)
exten = _8XXX,2,Congestion

Creamos la Ruta para el usuario de la Sede así:

[Ruta]
exten = _9XXX,1,Dial(IAX2/servidor B/${EXTEN : 1},30)
exten = _9XXX,2,Congestion

13.6. CREACION DE LAS TRONCALES IAX PARA LA CONEXIÓN ENTRE LAS CENTRALTAS DE LA EMPRESA BUSINESS STRATEGY LTDA. Y LA SEDE DE TRABAJO DEL PROYECTO

Ya creado los dos usuarios de los puntos a conectar ahora empezaremos a configurar la conexión entre las dos centralitas IPBX por medio del protocolo IAX que nos permite que los usuarios de los dos lugares puedan comunicarse entre sí, se usa el protocolo IAX porque es transparente a la NAT.

El Servidor Asterisk para la Empresa será Servidor B entonces:

Editamos el archivo iax.conf así:

[general]
bindport=4569
disallow = all
allow = gsm
language = es

;;Servidor B (Empresa)

[servidor A]
type = friend
context = default
secret = 0002
host = 190.96.169.40
qualify = yes

El Servidor Asterisk para la Sede será Servidor A entonces:

Editamos el archivo iax.conf así:

[general]
disallow = all
allow = gsm
language = es

;;Servidor A (Sede)

[servidor B]
type = friend
context = default
secret = 0003
host = 10.1.1.30

secret = 0003
qualify = yes

13.7. CREACIÓN DEL IVR

13.7.1. PLAN DE MARCADO

- Se desarrolló un plan de marcación que al digitar 400 reproduzca el mensaje welcome usando la aplicación Background (mensaje-reproducir) luego de reproducir el mensaje esperar 4 segundos que sea digitada la opción, 1 para extensión 400.

Solución:

Editamos el archivo extensions.conf del Servidor de la Empresa y agregamos en el contexto default lo siguiente:

```
[default]
;;inicio IVR
exten => _400,1,Answer()
exten => _400,2,Background(welcome)
exten => _400,3,Waitexten(4)
exten => _400,4,Hangup()

;;marcar extensiones
exten => 1,1,Dial(SIP/400)
```

- Se desarrolló un plan de marcación que al digitar 500 reproduzca el mensaje welcome usando la aplicación Background(mensaje-reproducir)

luego de reproducir el mensaje esperar 4 segundos que sea digitada la opción, 1 para extensión 500.

Solución:

Editamos el archivo extensions.conf del Servidor de la Sede y agregamos en el contexto default lo siguiente:

```
[default]
;;inicio IVR
exten => _500,1,Answer()
exten => _500,2,Background(welcome)
exten => _500,3,Waitexten(4)
exten => _500,4,Hangup()
;;marcar extensiones
exten => 1,1,Dial(SIP/500)
```

RECORDAR QUE: Para que todos los cambios tengan efecto debes hacer un reload, para ello se ejecuta:

```
# asterisk -r
> reload
> exit
```

13.8. CONFIGURACIÓN DEL SOFTPHONE (XLITE) PARA PERMITIR LAS LLAMADAS DESDE LA EMPRESA Y LA SEDE DEL PROYECTO.

Ahora se ejecuta el Setup eyeBeam.exe e instalamos el programa.

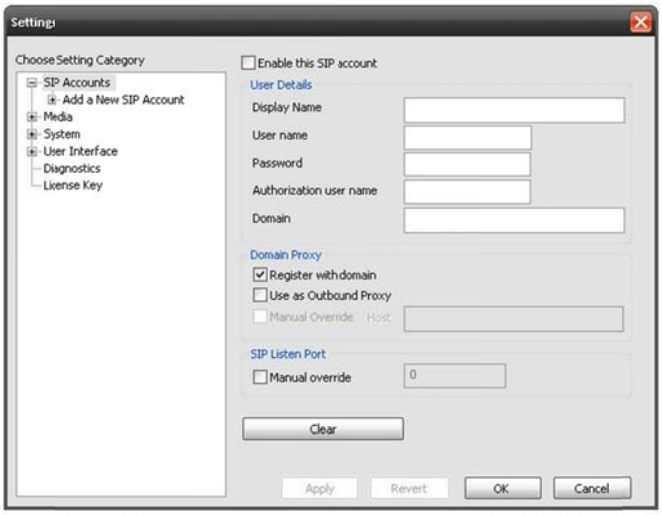
A continuación se configura el Softphone para la Empresa:

PASO 1

Después de instalar el teléfono eyeBeam, haga clic con el botón izquierdo sobre la pantalla del "softphone". Después haga clic en "Settings" para configurar.

PASO 2

Llenar los siguientes campos



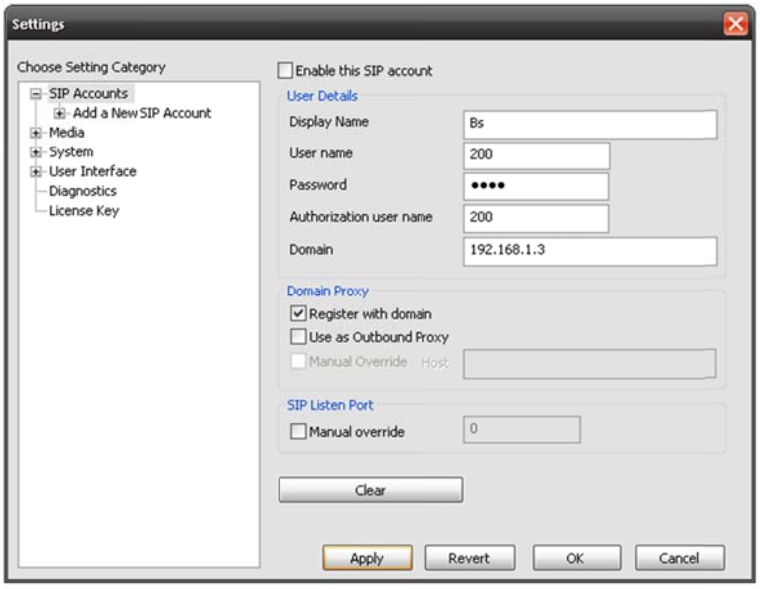
Display Name: Ingrese el nombre de la extensión creada.

User Name: Ingrese el número de teléfono que eligió para su extensión.

Password: Ingrese la contraseña que eligió para su extensión.

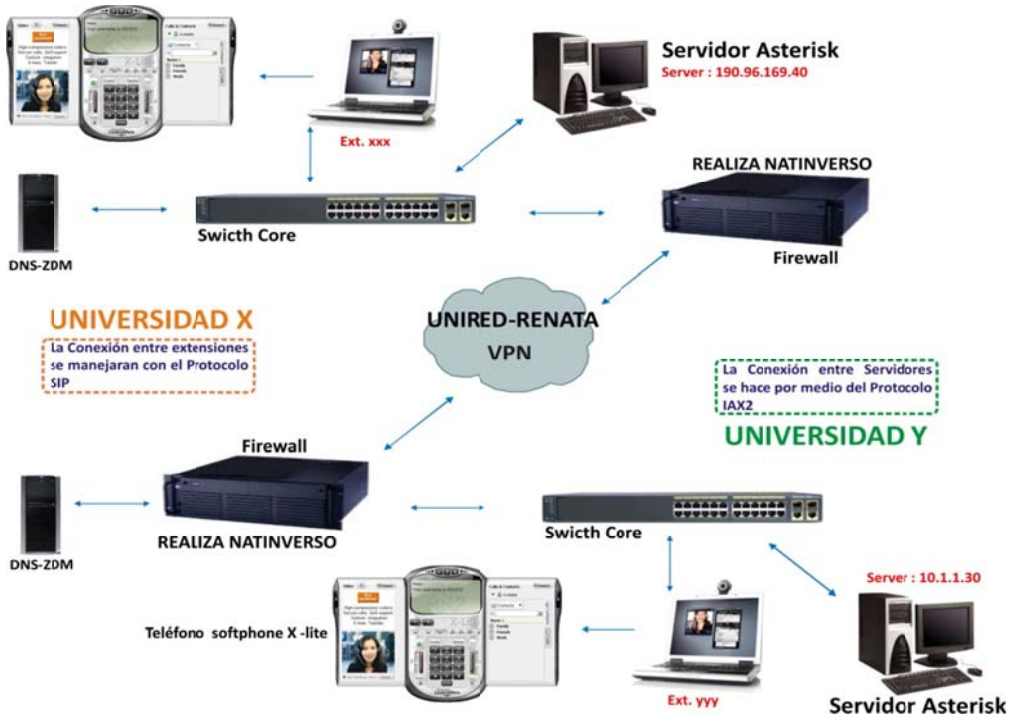
Authorization user name: Ingrese el número de teléfono que eligió para su extensión.

Domain: Dirección física del Servidor IPBX de la Empresa.



Para la configuración del softphone de la Sede de Trabajo seguimos los pasos que realizamos anteriormente utilizando los datos propios de la configuración de su extensión.

14. DISEÑO DEL PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED DE UNIVERSIDADES DE SANTANDER (UNIRED) Y LA RED NACIONAL UNIVERSITARIA (RENATA)



La figura 12 nos muestra el protocolo que se utilizará para las diferentes conexiones entre las Universidades de la red UNIRED y la red RENATA que permite la comunicación de forma gratuita entre las sedes obteniendo el intercambio de información académica e investigativa, como se observa la conexión se hará vía Internet y utilizáremos teléfonos Softphone con sus respectivitos auriculares que son las extensiones de cada sede y se conectarán mediante el protocolo SIP.

Cada sede manejara un Servidor Asterisk para conectarse entre sí mediante el protocolo IAX2 ya que este nos permite minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red IP, con particular atención al control y a las llamadas de voz y suministrando un soporte nativo para ser transparente a NAT.

Para el buen funcionamiento de las conexiones se necesito mapear y habilitar los puertos manejados por los protocolos SIP y IAX2, para ello se utilizo el dispositivo Firewall que realiza NATINVERSO y nos permite abrir los puertos 4569 (IAX2) y 5060 (SIP).

También la conexión se hace más segura por medio de una VPN ya que los paquetes viajan a través de infraestructuras públicas (Internet) en forma encriptada y a través del túnel de manera que es prácticamente ilegible para quien intercepte estos paquetes.

Aunque las redes que se conectan son de carácter privado el usuario que tenga el privilegio de manejarse por ellas puede obtener cualquier información por esta razón se implemento las VPN para asegurar los datos, también se implemento para los usuarios llamados RoadWarriors que se les permite conectarse por medio de PPP al servidor Asterisk de forma segura sobre una red privada o una red pública.

14.1. COSTO DE DISEÑO DEL MODELO DE INFRAESTRUCTURA PARA LA INTERCONEXIÓN ENTRE LA RED UNIRED Y LA RED RENATA

DISPOSITIVO	ESPECIFICACIONES	VALOR ($US)
 HP (HEWLETT-PACKARD) PROLIANT ML370 G5 5U TOWER SERVER	Servido Asterisk con procesador Intel Xeon E5430 Quad Core de 2.66 GHz, Memoria RAM DDR2 de 4 GB y Disco duro de 300 GB, manejando una capacidad de 66 extensiones.	1.779
 SOFTPHONE EYEBEAM	Es un software libre, maneja usuarios SIP y IAX2, Alta calidad de servicio (QoS), Seguridad vía TLS y SRTP, etc.	Free
 3COM 4500G	El 3Com Switch 4500G es un switch 10/100/1000 Ethernet agrupable en cluster que proporciona una conectividad de LAN segura y flexible, así como funcionalidades avanzadas	1.719

24-PORT SWITCH	optimizadas para voz tales como VLAN automática de voz y QoS.	
 FIREWALL (NAT-INVERSO)	El firewall es una computadora con el software de acceso libre MONOWALL que maneja las funciones de VPN, NAT y de protección de puertos para la telefonía.	292
 DNS – ZDM	Servidor DNS PowerEdge T100 maneja un procesador Intel Celeron 430 de 1.8GHz, 512K Cache, 800MHz FSB, Memoria de 1GB DDR2 y disco duro de 160 GB.	734
 Diadema IP		29
Total (US$)		**4.553**

Tabla 10 Costo de Diseño

14.2. VENTAJAS DE LA IMPEMENTACIÓN DEL PROTOTIPO DE INTERCONEXIÓN DE VOZ SOBRE IP ENTRE LA RED (UNIRED) Y LA RED NACIONAL UNIVERSITARIA

- ✓ Independencia:
  - o Autonomía de gestionar su centralita mediante una interfaz web.
  - o Al ser un sistema abierto dispone una independencia total tanto del proveedor como de las operadoras telefónicas.

- ✓ Funcionalidad: Asterisk dispone de todas las funcionalidades de las grandes centralitas propietarias (Cisco, Avaya, Alcatel, Siemens, etc.). Desde las más básicas (desvíos, capturas, transferencias, multi-conferencias,…) hasta las más avanzadas (Buzones de voz, IVR, CTI, ACD…).

- ✓ Escalabilidad:
  - o El sistema puede dar servicio desde 10 usuarios en una sede de una pequeña empresa, hasta 10.000 de una multinacional repartidos en múltiples sedes.
  - o Le permite ir migrando extensiones de su centralita antigua progresivamente.
  - o Posibilidad de aumento de extensiones sin costo de infraestructura.
  - o No es un sistema propietario con el consiguiente ahorro en licencias.
- ✓ Competitividad en coste: No solo por ser un sistema de código abierto (Open Source) sino gracias a su arquitectura hardware: utiliza plataforma servidor estándar (de propósito no específico) y tarjetas PCI para los interfaces de telefonía, que por la competencia del mercado se han ido abaratando progresivamente.

- ✓ Interoperatibilidad y Flexibilidad**:** Asterisk ha incorporado la mayoría de estándares de telefonía del mercado, tanto los tradicionales (TDM) con el soporte de puertos de interfaz analógicos (FXS y FXO) y RDSI (básicos y primarios), como los de telefonía IP (SIP, IAX2, H.323, MGCP, SCCP/Skinny). Eso le permite conectarse a las redes públicas de telefonía tradicional e integrarse fácilmente con centralitas tradicionales (no IP) y otras centralitas IP.

- ✓ Es más barato si se considera que no requiere del pago de un cargo fijo, como la telefonía convencional. Sólo se necesita una buena conexión a Internet y los equipos adecuados para ya estar hablando a cualquier parte del mundo.
- ✓ Se estima que el costo se reduce en alrededor de un 70%, por lo que el monto depende específicamente de lo que ofrezca el mercado y no del tiempo que dure una determinada llamada.

  - o Ejemplo de tarifas ($COP)
    - Colombia – Bogotá 39
    - Estados Unidos 25
    - España – Fijo 30
    - España – Móvil 220
    - Venezuela – Fijo 40
    - Venezuela – Móvil 160

- ✓ Aunque todavía no es una tecnología demasiado expandida en nuestro país, cada vez son más los usuarios que descubren sus ventajas y que han comenzado a implementar el servicio ya sea en sus hogares o sus lugares de trabajo.
- ✓ Se espera que para el año 2010, el 25% de las llamadas realizadas en todo el mundo se efectúen a través de la telefonía IP, situación que se cree irá aumentando con los años.

- ✓ Asterisk es un software de PABX que usa el concepto de software libre (GPL) tan difundido y usado actualmente.

15. RECOMENDACIONES

- ✓ Se recomienda instalar el servidor Asterisk en un equipo destinado para esta labor, ya que no es conveniente compartir los recursos con otros sistemas operativos en otras particiones.

- ✓ El proyecto se realizo basado en la conexión vía internet gracias a los protocolos SIP y IAX2, se recomienda implementar las conexiones por medio de la Red Telefónica Publica Conmutada (PSTN) utilizando el proveedor de telefonía IP, las tarjetas (FXS y FXO) y el software Dahdi que se implementan en el Servidor Asterisk y que permitirán sacar llamadas no solo por internet sino también a teléfonos convencionales.

- ✓ Realizar la conexión con la red CLARA (Cooperación Latino Americana de Redes Avanzadas) y la red ALICE (América Latina Interconectada con Europa) permitiendo construir el enlace con las redes internacionales de alta velocidad y los centros de investigación más desarrollados del mundo.

16. CONCLUSIONES

- De acuerdo con la investigación sobre las diferentes herramientas de código libre se escogió para crear la conexión el software Asterisk 1.4 que permite una excelente configuración e instalación de la central IP-PBX y el sistema operativo Debian de Linux con Kernel 2.6, siendo el sistema operativo de mejor resultado.

- El protocolo SIP se escogió para las conexiones internas porque permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y el protocolo IAX2 para las conexiones entre centralitas Asterisk ya que permite minimizar el ancho de banda utilizado a través de la red IP y suministra un soporte nativo para ser transparente a NAT.

- Al analizar la infraestructura de la red UNIRED y RENATA se encontró que el cableado estructurado esta certificado y es conveniente para la interconexión entre ellas con un gran índice de calidad de servicio.

- Se modelo el prototipo de la Plataforma de Voz sobre IP capaz de ofrecer servicios de telefonía y voicemail a extensiones VoIP basadas en protocolo SIP permitiendo la comunicación de la red UNIRED con la red RENATA el cual permitirá el intercambio de información académica e investigativa. Las extensiones conectadas a la centralita, pueden comunicarse de forma totalmente gratuita.

- El diseño de la IPBX se ha basado en la utilización de herramientas GNU con la consecuente reducción de costos. Gracias a las licencias GPL de Linux y Asterisk fue posible la interconexión de las Universidades con las mismas características de las actuales centralitas a un precio más económico.

- Las centralitas se encargan de establecer la conexión entre las distintas terminales, también ofrecen servicios de valor agregado como voicemail, música en espera y operadora virtual entre otras.

- Se realizo el proyecto utilizando el protocolo SIP (Troncales y Extensiones) pero al hacer las actividades se presentaron inconvenientes en la NAT cuando se necesitaba conectar dos centralistas Asterisk por ello se realizo el prototipo utilizando troncales IAX y Extensiones SIP.

17. ANEXO SIP.CONF

Se anexa la prueba de conexión que se realizo de forma virtual para el desarrollo del proyecto:

La configuración del prototipo para interconexión de las Universidades a través de troncales SIP's, se hizo con Xlite y Xlite eyeBeam (Softphone y teléfono Grandstream).

Para ello se utilizaron maquinas virtuales con VMware*Station sobre Centos donde se configuraron las extensiones de los clientes para efectuar la marcación a través de la troncal Sip.

Se crea una red interna con el VMware*Station que permitía comunicar las dos maquinas Centos clientes a través de troncales Sip con la red 10.10.0.1 con el server principal SIP.

Las extensiones utilizadas para el prototipo son: 400 y 500, la extensión 400 es el Xlite y la extensión 500 es el teléfono IP.

La configuración del contexto en forma general del archivo SIP.conf en cada una de las maquinas:

```
[general]
context=default                 ; contexto por defecto para las llamas  entrantes
realm= class.digium.com         ; ámbito para autentica el texto
bindport=5060                   ; Puerto UDP  a utilizar
bindaddr=0.0.0.0                ;Cualquier dirección IP a conectar por defecto escucha
todas  (0.0.0.0 binds to all)
srvlookup=yes                   ;permite las búsquedas de DNS y Srv
```

```
disallow=all                ;primero rechazar todos los codecs
allow=ulaw                  ;codecs permitidos ordenados por preferencia
allow=gsm
language=es                 ;idioma por defecto
```

Se crea las extensiones de los clientes:

```
[400]                       ;Softphone Xlite
type=friend                 ;enviar y recibir llamadas
qualify=yes                 ;mandar ping para que este refrescados los teléfonos
nat=yes                     ;para hacer nat con un firewall
callerid="Telefono IP" <100>  ;Aquí los teléfonos con display le digo me muestre el
nombre y la extensión
host=dynamic                ;registre cualquier teléfono
secret=100                  ;clave secreta
context=longdistance        ;Contexto tomado dial plan archivo extensions.conf
mailbox=100@default         ;agrego buzón de mensajes para la extensión

[500]                       ; Teléfono IP grandstream
type=friend                 ;Enviar y recibir llamadas
qualify=yes                 ;mandar ping para tener refrescados los teléfonos
nat=yes                     ;para ser NAT con un firewall
callerid="X-Lite" <200>     ;Aquí los teléfonos con display le digo me muestre el
                            nombre y la extensión
host=dynamic                ;registre cualquier teléfono
secret=200                  ;clave secreta
context=local               ;contexto tomado dialplan archivo extensions.conf
mailbox=200@default         ;Agrego buzón de mensajes para la extensión
```

****

En esta sección del Sip.conf se colocaron 3 maquinas virtuales instaladas con Centos todas conectadas a través de una red internet con VMware*Station.

La troncal que recibe es decir el server Sip debe contener las iP'S de las otras maquinas clientes que permiten crear la troncal como se muestra a continuación.

Server Asterisk principal que conecta las troncales SIP de los clientes universidad 1 y universidad 2:

Universidad 1

```
[5550001]
type=friend
context=users
disallow=all
allow=gsm
allow=ulaw
allow=alaw
host=192.168.1.119
insecure=invite,port
username=5550001
fromuser=5550001
secret=5550001
canreinvite=no
qualify=yes
nat=no
```

Universidad 2

[5550002]
type=friend
context=users
disallow=all
allow=gsm
allow=ulaw
allow=alaw
host=192.168.1.156
insecure=invite,port
username=5550002
fromuser=5550002
secret=5550002
canreinvite=no
qualify=yes
nat=no

18. BIBLIOGRAFIA

- CAPACITA-T (www.capacita-t.com). Trixbox Modulo I: Instalación y Configuración Básica. Septiembre 2008.

- GONÇALVES, Flavio E. Asterisk PBX Guía de la configuración: Como construir y configurar un PBX con software libre Asterisk 1.4. Primera Edición, Enero 2007.

- KUNTHUR y BEPPO TRAINING. Asterisk Training: Configuración y Administración de VoIP sobre Asterisk. Noviembre 2008.

- MEGGELEN, Jim Van. MADSEN, Leif. y SMITH, Jared. Asterisk: The future of Telephony. Second Edition, August 2007.

- MICCHIELLI, Lucas. REGGIANI, Federico. Revista NENOTEO. En: Guía de Instalación de Asterisk: La Centralita Telefónica Total. Nº 6, Febrero del 2007.

- SALMERÓN, Sandra. TELEFONÍA EN REDES EHAS CON ASTERISK (V.2.0). Madrid: Universidad Carlos III, 20 Junio de 2005.

- SHEET, Kris. ESTRADA, Jimmy T. GARCIA, Marcelo y SAAVEDRA, Dany. Asterisk en Español. Versión 1, Abril 2005.

- SPENCER, Mark. ALLISON, Mack. RHODES, Christopher. The Asterisk Handbook Version 2. March 2033.

o VIEGAS, Eduardo Federico y CORREA, Facundo Hernán, Integrantes de Asterio Argentina. Manual para Administradores y usuarios de Trixbox, el Asterisk sin consola: Asterisk Desconsolado.