



UNIVERSIDAD NACIONAL TECNOLÓGICA DEL CONO SUR DE LIMA  
(UNTECS)

PROPUESTA PARA LA IMPLEMENTACIÓN DE LA TELEFONÍA IP COMO  
COMPLEMENTO EN LA COMUNICACIÓN DIGITAL TETRA EN  
CAMPAMENTOS MINEROS

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL TÍTULO DE  
INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER  
CHRISTIAM CARLOS SUYBATE RACCHUMI

LIMA-PERÚ

2014

#### **DEDICATORIA**

A mi familia, mis  
padres y mi  
hermana, mis  
Amigos, que con su  
apoyo incondicional  
siempre me  
alientan.

## **AGRADECIMIENTO**

Agradezco a los catedráticos de la UNTECS, en especial a los de la Escuela de Ingeniería Electrónica y Telecomunicaciones por haberme preparado con los conocimientos suficientes para ser un profesional que sirva mejorar la sociedad en la que vivimos.

## INTRODUCCIÓN

El presente trabajo de investigación lleva por título “PROPUESTA PARA LA IMPLEMENTACIÓN DE LA TELEFONÍA IP COMO COMPLEMENTO EN LA COMUNICACIÓN DIGITAL TETRA EN CAMPAMENTOS MINEROS”, para optar el título de Ingeniero Electrónico y Telecomunicaciones, presentado por el alumno Christiam Carlos Suybate Racchumi.

Se trata de que la comunicación se estandarice y unifique siendo de una utilización accesible sin la necesidad de tantos equipos, simplificarla de tal manera que un gerente pueda estar comunicado desde su oficina con el ingeniero de campo siendo esta comunicación eficaz y eficiente en todo lugar y hacia todo lugar; mantener un entorno de comunicación estable y confiable, permitiendo así la rápida y oportuna reacción de las áreas indicadas en caso de cualquier novedad. Concretándose esto en un entorno de trabajo confiable en que el trabajador como el jefe se sienta confiado que las reacciones se den de la mejor manera y en el tiempo oportuno mejorando la eficacia en el área de trabajo de la ingeniería tanto de campo como de soporte desde la oficina.

La estructura que hemos seguido en este proyecto se compone de 3 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del diseño.

## CAPITULO I

### PLANTEAMIENTO DEL PROBLEMA

#### 1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

En el contexto de un campamento minero siendo la comunicación una necesidad prioritaria y obligatoriamente confiable y no contando con la facilidad de una comunicación de línea baja (celular) en todo el campamento, y teniendo como solución al problema una comunicación troncal digital TETRA a nivel de campo y oficinas o simplemente a algunos cargos de relevo, la comunicación no siempre es completa o precisa ya que por el costo de cada equipo no todas las personas pueden ser dotadas de un equipo cada una, o simplemente por ser una radio de una área tiene que estar en la oficina del área y cuando hay una novedad y se busca a una persona puntual, esta no está en su oficina, haciendo de esto un problema significativo ya que se gasta tiempo. Y en una emergencia o en una toma de decisión inmediata este letargo en la comunicación tendrá una consecuencia grave.

#### 1.2 JUSTIFICACIÓN DEL PROBLEMA

Siendo la minería uno de los rubros económicamente fuertes invierten en lo que denominan tolerancia cero; cero accidentes, incidentes, desvíos, alcohol, etc.; dependiendo esto de una comunicación oportuna y directa con las personas encargadas, dando así la confiabilidad del trabajo en el campamento minero, la comunicación directa en el campamento de una necesidad se convierte prácticamente en una obligación que tendrá que ser robusta, práctica y accesible en todo el campamento; todo esto le dará a la

minera el respaldo necesario para las certificaciones que quiera obtener. Todo esto en su conjunto hace que los riesgos en el trabajo se minimicen elevando a la empresa a un estatus superior de presentación como marca.

### 1.3 DELIMITACIÓN DE LA INVESTIGACIÓN

**Teórica:** Comunicación Troncalizada TETRA – ASTERISK (SIP)

**Espacial:** Campamento minero.

**Temporal:** Comprende el periodo Enero 2014 a Abril 2014

### 1.4 FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede hacer más accesible la comunicación en todo momento y en todo lugar en un campamento minero que utilice la comunicación focalizada TETRA, siendo esta robusta y factible?

### 1.5 OBJETIVO

Implementar los servicios necesarios en los servidores adecuados para complementar la comunicación digital tetra con la telefonía IP basada en Asterisk para que la comunicación sea accesible, rápida y eficiente.

## **CAPITULO II**

### **MARCO TEÓRICO**

#### **2.1 ANTECEDENTES**

A lo largo de la investigación, se encontraron varias tesis que sirvieron de ayuda para el presente trabajo, entre ellas están:

Br. Rodríguez G., Reinaldo J. “ESTUDIO DE PROPAGACIÓN Y COBERTURA DEL 60% DEL SISTEMA DE RADIO COMUNICACIONES BAJO PROTOCOLO TETRA PARA LA ALCALDÍA DEL DISTRITO METROPOLITANO DE CARACAS EN SU MIGRACIÓN DESDE EL ESTÁNDAR APCO25”, este trabajo propuesto para la Alcaldía del Distrito Metropolitano de Caracas, dicho sistema busca ofrecer servicios de comunicación móvil troncalizada bajo el protocolo europeo TETRA (Radio Troncalizado Terrestre por sus siglas en inglés) a las dependencias y cuerpos adscritos a la Institución a lo y ancho de la ciudad capital. Teniendo como concluyente “que es realizable teniendo las precauciones necesarias en las colocaciones de la estaciones bases y siempre teniendo el análisis de coberturas muy al pendiente”.

Víctor Hugo López Chalacán. “ANÁLISIS DE LA PAQUETIZACIÓN DE VOZ SOBRE IP EMPLEANDO EL PROTOCOLO DE INICIO DE SESIONES SIP CON BACK TO BACK USER AGENT (B2BUA) EN UNA APLICACIÓN SOBRE REDES WI-FI” busca explotar la red de redes (internet) haciendo utilización del protocolo SIP que contiene una entidad lógica denomina Back to Back User Agent (B2BUA), encargada del control, gestión de llamadas entre

usuarios SIP, interconexión de red, transcodificación entre los puntos terminales de la llamada, entre otros. Concluyendo del estudio, “Del estudio realizado se determinó que el Protocolo SIP es más simple que otros protocolos, y mucho más adecuado para VoIP y otras aplicaciones de internet. Por lo tanto más y más empresas y organizaciones alrededor del mundo eligen equipos compatibles con SIP. La elección de productos basados en el estándar SIP asegura que se pueden mezclar productos de diferentes fabricantes y que va a ser parte del mundo VoIP en el futuro”.

Jesús Martín Caballero Basto. “IMPLEMENTACIÓN DE UNA RED (VOIP) A TRAVÉS DE SOFTWARE LIBRE EN EL DESARROLLO DE UNA PEQUEÑA CENTRAL TELEFÓNICA”, basándose en la vida actual se sabe que si no hay una correcta comunicación entre los niveles que conforman cualquier estructura empresarial, simplemente no funciona como se espera, es por esto que las empresas actuales necesitan de una estructura de comunicación a bajo precio, eficiente y acorde a sus necesidades. Encontrando como solución “el Asterisk que cambia todo siendo esta una tecnología abierta que proporciona un estándar de comunicaciones VoIP, por lo que no se está sujeto a las limitaciones de ningún fabricante, se está en libertad para desarrollar las innovaciones que se requieran y en general no se impone ningún límite”.

Jhonny Christian Girón León. “ANÁLISIS DEL ESTÁNDAR DE RADIO TRONCALIZADO DIGITAL TETRA (Terrestrial Trunked Radio) Y DE SU POSIBLE APLICACIÓN EN EL ECUADOR” se centra principalmente en lo que se refiere al protocolo de comunicaciones (reconocimiento de cada uno de los procesos realizados desde la capa física AI1 hasta llegar a la capa de red AI3), interconexión con otras redes importantes a través de sus gateways (PSTN, PABX, ISDN, Redes IP). Además se analiza el esquema de direccionamiento utilizado en TETRA para interconectarse con otras redes TETRA a través de la interfaz ISI (Interfaz Inter -Sistema). Concluyendo que “el sistema TETRA posee ventajas en menor sensibilidad a ruido al igual que posee detección y corrección de errores, utilización de vocoders (voz digitalizada), teniéndolo en prioridad para moderniza su comunicación siendo está segura y confiable”.



Jorge Armando Gómez Wilches. “ESTUDIO Y DISEÑO DE UNA RED DE TELEFONIA DE VOZ SOBRE IP PARA PLATAFORMA SIGLO XXI”, En el capítulo de diseño de la red se muestra la topología red existente, los diferentes dispositivos y el estado en el que se encuentran, la distribución de los equipos de la red telefónica y se estudian las consecuencias y los problemas que se puedan presentar en cuanto a calidad de servicios y la forma de asegurar un buen QoS. Teniendo como resultado “conocimiento de los conceptos básico y las generalidades de este tipo de red sobre voz IP demostrando la capacidad de conocimiento y recursividad adquirida en la etapa de formación de pregrado, y el conocimiento de los tipos de protocolos que se utilizan en una comunicación de voz IP”.

## **2.2 BASES TEÓRICAS**

### **2.2.1 EL ESTÁNDAR TETRA.**

El sistema de Radio Troncalizado Terrestre (TETRA) es un estándar elaborado y definido por la ETSI (Instituto Europeo de Estándares para las Telecomunicaciones) para reglamentar un sistema de radio móvil troncalizado y digital para el uso en la Unión Europea que permitiera la unificación de las soluciones existentes e incentivara la convergencia de esfuerzos de los distintos fabricantes. TETRA es una solución lo suficientemente abierta y definida para garantizar la interoperabilidad entre fabricantes y por ende facilitar la sana competencia y compatibilidad entre los mismos.

Con las banderas de apertura y compatibilidad, la ETSI busca que TETRA se convierta en el estándar más aceptado mundialmente para soluciones de Radios Móviles Profesionales, algunos de los mercados que TETRA busca explotar son:

- Seguridad pública.
- Sistema de ambulancias.
- Transporte público y privado.
- Aplicaciones militares.

- Comunicaciones gubernamentales.
- Comunicaciones para industrias medianas y grandes.

Muchas de las características de TETRA son heredadas directamente de la solución europea para telefonía celular GSM (Sistema Global de Comunicaciones Móviles por sus siglas en inglés), en estos términos TETRA también emplea multiplexación TDMA (Acceso Múltiple por División de Tiempo por sus siglas en inglés) en su acceso y se basa en la amplia definición de las interfaces involucradas para lograr la interoperabilidad entre fabricantes. Además es un sistema totalmente digital, donde la voz es codificada y decodificada en los extremos de la comunicación y manejada como data digital en el trayecto entre ambos. TETRA es capaz también de manejar transmisión de datos abriendo las posibilidades de múltiples aplicaciones adicionales.

#### 2.2.1.1 Estructura de red.

El sistema TETRA maneja una estructura de tipo celular en la que cada estación base atiende un área específica y todas las peticiones de llamadas que en ésta se den. Un esquema de la estructura de un sistema TETRA genérico es mostrado en la Figura 2.1. Entre los elementos más resaltantes de la estructura de TETRA se enumeran:

- Estación Base (BS).

También conocida como Radio Base es el elemento de red que proporciona la interfaz de aire empleada para brindarles comunicación a los equipos terminales en aéreas de servicios denominadas celdas. Posee una conexión con el nodo de conmutación que la maneja mediante un enlace de 2 Mbps.

- Nodo de Conmutación y Control (SCN).

El SCN es el encargado de manejar las funciones de troncalizado mediante la interconexión y manejo de varias BS,

terminales de despacho e interfaces con redes externas (PBX, PSTN, RDSI, etc.), además permite su conexión con otras SCN mediante topologías de malla o anillo. Cuando existe más de un SCN es necesario la utilización de un H-SCN (SCN de tipo Home o Local), donde se ubiquen las bases de datos HLR

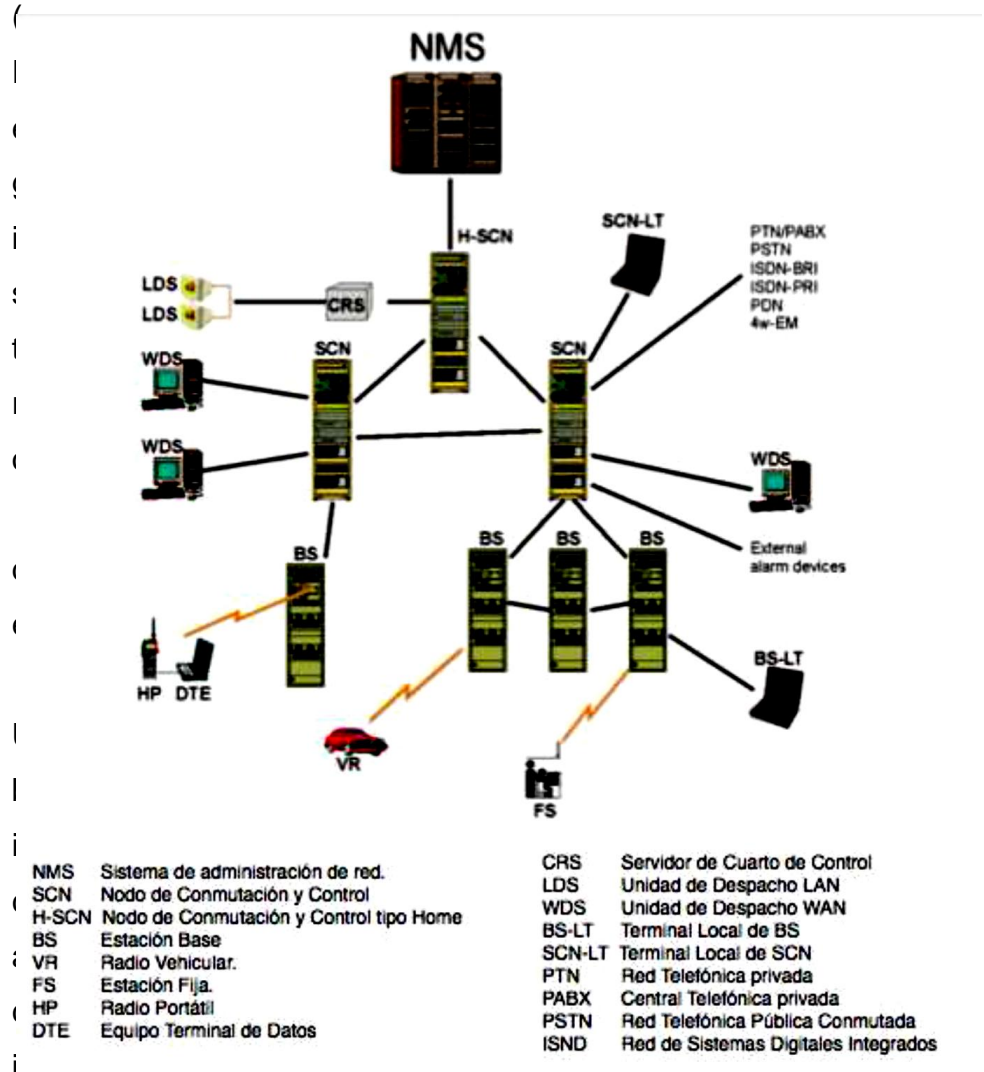


Figura 2.1 Estructura de Red TETRA. Tomado de "OTE Tetra Base Station 400T Technical Handbook" por OTE, 2004.

- Sistema de Administración de Red (NMS)

El NMS permite el manejo remoto de un determinado número de SCNs, permitiendo centralizar algunas funciones de monitoreo y control del sistema, es el nivel más alto de administración de la estructura TETRA y está formado básicamente por un servidor y varias interfaces gráficas para usuarios administradores.

- Terminales de comunicación.

Estos son los terminales con los que los usuarios del sistema pueden realizar llamadas, pueden ser fijos, portátiles o móviles. Los terminales TETRA tienen la capacidad de conmutar entre varios modos de operación; ya sea al cambiar entre modalidades half-duplex y full-duplex, hacer llamadas individuales o de grupo y conmutar entre métodos de comunicación definidos por el estándar, en el que permitiría incluso su operación de manera independiente cuando exista ausencia de la BS, el SCN o ambos.

- Terminales locales (LT).

Estos terminales son empleados en las premisas de los elementos de red para configurarlos y realizar monitoreo local de su funcionamiento, pueden estar ubicados junto a los equipos BS (BS-LT) y a los SCN (SCN-LT).

- Terminales de despacho.

Son ubicaciones desde la que un operador puede tener acceso al sistema, estableciendo comunicaciones de voz y datos con cualquier terminal o grupo de terminales, además de contar con una interfaz de monitores y funciones de administración. Estos terminales pueden tener conexiones de tipo LAN o WAN con los elementos del sistema.

- Interfaces de conexión.

El sistema TETRA permite que los SCN puedan conectarse a redes externas mediante interfaces que sirven de puertas de enlace para permitir funciones avanzadas como el establecimiento de llamadas telefónicas, transmisión de datos, consultas a bases de datos e incluso la conexión a Internet.

#### 2.2.1.2 Métodos de comunicación.

Por defecto, TETRA es un protocolo troncalizado y se beneficia de las características de esta tecnología, pero conscientes que debido a la fuerte dependencia que tienen los móviles a la BS más cercana, los desarrolladores del estándar incluyeron en sus características básicas funcionalidades de radiocomunicación convencional. En este sentido TETRA presenta varios modos de operación.

- Modo de Operación Troncalizado (TMO)

Este es el modo principal de operación del protocolo, requiere de la presencia de al menos una BS para poder funcionar y se basa en la utilización de la Interfaz de Aire principal (AI) descrita por la ETSI en la norma EN-300 392-2. Todos los móviles de una celda se comunican con los demás a través de la BS para hacer llamadas tanto individuales como de grupo compartiendo de forma dinámica los canales disponibles.

- Modo de Operación Troncalizado Voz y Datos (TMO- V+D)

Básicamente se comporta como el anterior pero emplea equipos de red y de acceso que permiten la transmisión de datos en conjunto con la voz para alcanzar velocidades de hasta 29 Kbps.

- Modo de Operación Directo (DMO)

Con el modo directo el estándar TETRA permite la comunicación entre terminales más allá del área de cobertura. La ETSI a través de varias recomendaciones y regulaciones, estandarizó este modo de operación para garantizar que cualquier móvil TETRA pueda funcionar independientemente de si se encuentra o no dentro de la sombra de una BS.

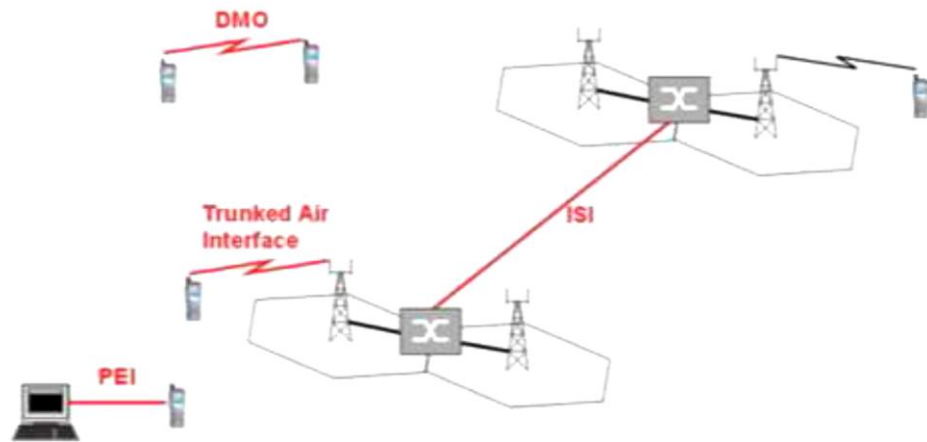
Las normativas de funcionamiento de DMO permiten distintas formas de complementación de llamadas, en primer lugar permite la realización de llamadas individuales o de grupo sin la presencia de BS alguna, simulando así un sistema convencional. También permite que dos móviles se comuniquen aún al superar su propia cobertura individual siempre que entre ellos exista algún equipo de enlace, para esto la mayoría de los equipos móviles a ser portados por vehículos automotores presentan características ya sea de repetidor, permitiendo el enlace de 2 móviles sin conexión directa o de puerta de enlace funcionando como interfaz entre un móvil fuera de cobertura y una BS.

- Funcionalidad de Independencia de las Estaciones Base.

Además de los modos de operación en los que el estándar hace un máximo esfuerzo por no perder comunicación aún y cuando no exista una BS, TETRA busca llevar el concepto de independencia y robustez del servicio hasta los últimos niveles, para esto el estándar permite que si en determinado momento un BS pierde su comunicación con el SCN que la maneja, automáticamente podrá hacerse cargo del manejo y control de las funcionalidades de troncalización de la celda que domina, logrando que todos los usuarios presentes en la celda puedan comunicarse de manera eficiente.

### 2.2.1.3 Interfaces.

Para garantizar la interoperabilidad entre fabricantes el estándar define varias interfaces (ver Figura 2.2) que deben poseer



estáticas bien definidas y que impiden la presentación de soluciones cerradas o propietarias que vayan en contra de la apertura de TETRA. Las principales interfaces definen la conexión entre terminales funcionando en modo DMO, entre los terminales y las BSs en modo TMO y por último entre distintos SCNs.

**Figura 2.2 Interfaces del Estándar TETRA.** Tomado de “OTE Tetra Base Station 400T Technical Handbook” por OTE, 2004.

- Interfaz de aire.

La Interfaz de Aire (AI) es la más importante dentro del estándar, pues reglamenta la forma en cómo se realiza la comunicación entre el terminal móvil y la estación base. Esta interfaz es descrita en la norma ETSI EN-300 392-2 de donde extraen las siguientes características.

- Acceso.

La tecnología de acceso utilizada por TETRA es el Acceso Multiplexado por División de Tiempo (TDMA) empleando 4 intervalos de tiempo por cada portadora de 25kHz de ancho de banda y una estructura que se

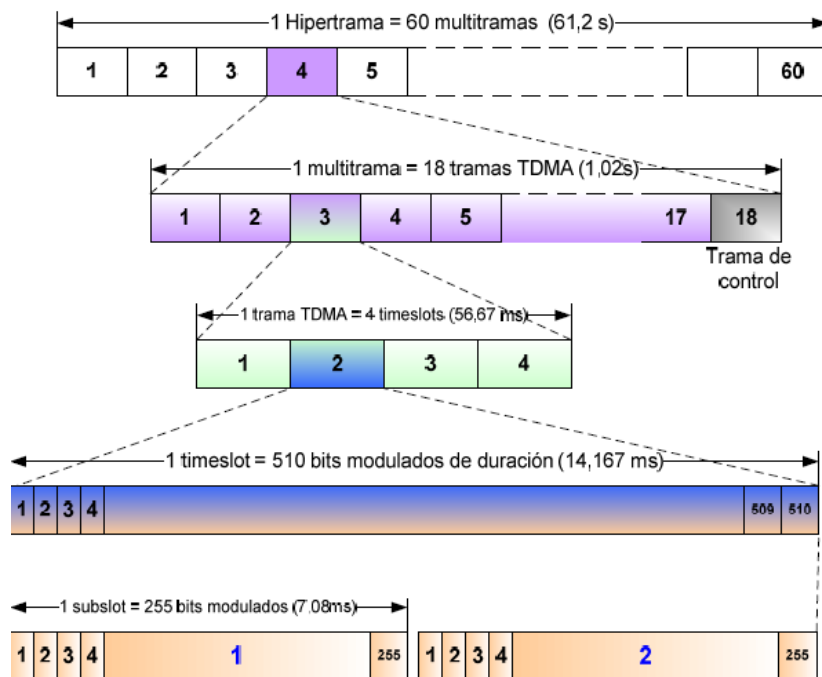
compone de tramas, multi- tramas e híper-tramas tal y como la que se presenta en la Figura 2.3.

- Modulación.

Para dar libertad a los fabricantes en el diseño de sus soluciones, TETRA permite la utilización de varios tipos de modulación. En primer lugar se utiliza Modulación en Cuadratura Diferencial por Desplazamiento de Fase (DQPSK) en sus variantes de  $\pi/4$  y  $\pi/8$  para modular canales de 25 kHz y en segundo lugar también se permite modulación de amplitud en cuadratura en sus versiones de 4-QAM, 16-QAM y 64-QAM que podrán trabajar con canales de 25, 50, 100 y 150 kHz.

- Frecuencias

El estándar plantea mediante la norma ETSI EN-100 392-15 parámetros para definir posibles planes de frecuencias para sistemas TETRA dentro un rango que va desde 100 y hasta 900 MHz. La ETSI define un diseño de doble banda con una banda inferior para el enlace donde transmite la móvil y recibe la BS y una banda superior para el caso contrario.





**Figura 2.3 Estructura de trama TETRA.** Tomado de la recomendación “ETSI EN300 392-2 V3.2.1” por ETSI, 2007.

En la búsqueda de minimizar la cantidad de BS para implementar un sistema TETRA, los fabricantes proponen la utilización de bandas de frecuencias relativamente bajas para las manejadas tradicionalmente en sistemas móviles en Europa. Las frecuencias ubicadas entre 380 y 470 MHz son las preferidas, con un separación entre las bandas superior e inferior de 10 MHz y empleando canales de 25kHz modulados en fase. En la Tabla 2.1 se presentan las principales bandas u

Banda	Enlace Móvil → BS		Enlace BS → Móvil	
380 - 400	380 - 385	385 - 390	390 - 395	395 - 400
410 - 430	410 - 415	415 - 420	420 - 425	425 - 430
450 - 470	450 - 455	455 - 460	460 - 465	465 - 470
800 - 870	806 - 815	815 - 825	851 - 860	860 - 870
	Banda Baja	Banda Alta	Banda Baja	Banda Alta

a

das por los fabricantes de TETRA.

Tabla 2.1. Principales bandas de frecuencia para TETRA. Elaborado con datos tomados de la recomendación “ETSI TS 100 392-15” por ETSI, 2004

- Interfaz DMO

Las características técnicas de esta interfaz son idénticas a las de la AI con la salvedad del uso de los slots de tiempo. DMO

permite solo una llamada por canal en la modalidad normal, donde se emplean dos intervalos de tiempo para el tráfico y dos como espacio de guarda y hasta dos llamadas en el modo de ahorro de frecuencia, donde cada llamada usa dos intervalos.

- Interfaz ISI

La Interfaz de Interconexión de Sistemas busca estandarizar la forma como dos o más sistemas TETRA independientes se pueden conectar, esto busca garantizar la compatibilidad entre fabricantes y la interoperabilidad entre sistemas sin importar su ubicación y estructura. Normalmente esta interfaz se ubica entre dos SCNs y se basa en una serie de parámetros y requerimientos protocolares presentados por el ETSI mediante la norma EN-300 392-03.

- Interfaz PEI

La Interfaz de Equipos Periféricos se emplea para conectar los equipos terminales sean fijos, portátiles o móviles con dispositivos extra como computadoras o unidades de monitoreo especializado. Es una interfaz de tipo punto-punto que busca proteger en todo momento al consumidor evitando las interfaces propietarias. Además esta interfaz permite el uso de aplicaciones extra como el acceso a internet o la consulta de bases de datos propias. Sus características técnicas se describen en la norma ETSI EN-300 392-05.

- Otras interfaces.

El resto de las interfaces empleadas por el sistema no están estandarizadas y queda a juicio del fabricante su diseño y escogencia. La forma en cómo se conectan las unidades locales y de despacho, los sistemas de control o la conexión entre las BSs y los SCNs podrán ser propietarias, es decir el comprador

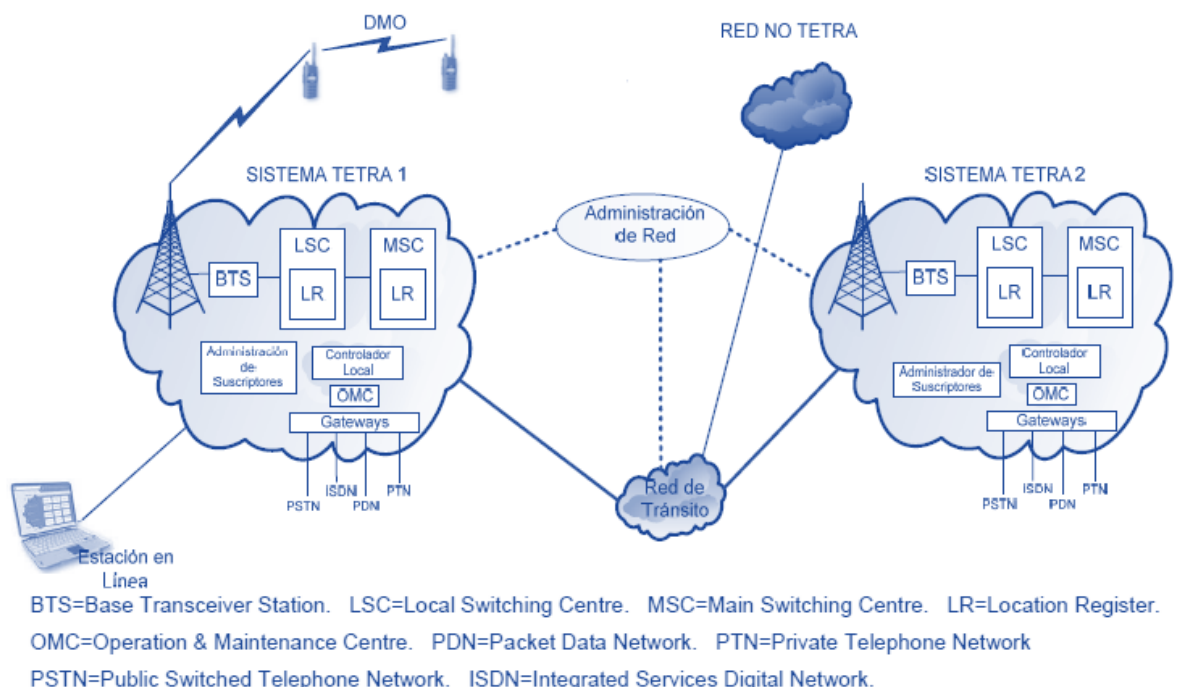
estará obligado a usar BSs y SCNs del mismo fabricante, un ejemplo:

- Infraestructura de Administración y Conmutación (SwMI)

Es el componente básico dentro de la red TETRA, comprende los aspectos necesarios para la administración, conmutación, networking y elementos no estandarizados de la red. Los beneficios de la no estandarización es que se deja a los fabricantes del mercado, en libertad de implementar soluciones rentables para la red. SwMI comprende hasta seis subsistemas los cuales son:

- Estación Móvil
- Estación en Línea
- Estación Móvil en Modo Directo
- Gateway
- Unidad de Administración de la Red
- Red Individual TETRA

Estos elementos se interconectan a través del uso de interfaces específicas. SwMI proporciona un dominio de red común para estos componentes. La configuración



de SwMI se muestra en la Figura 2.4.

**Figura 2.4 Configuración SwMI**

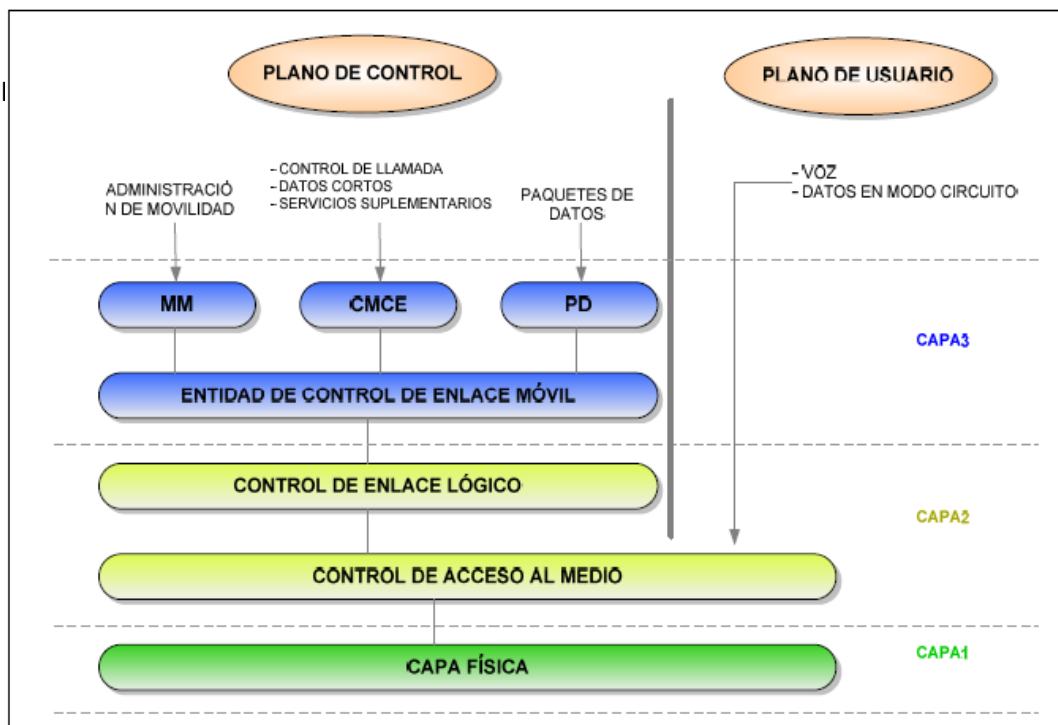
#### 2.2.1.4 Opciones y tecnologías compatibles.

El protocolo TETRA está pensado para su compatibilidad con múltiples redes y tecnologías, permite la conexión Internet desde los equipos terminales y la configuración de VPN (Redes Privadas Virtuales) para el acceso a servidores y aplicaciones propias así como el establecimiento de llamadas telefónicas full-dúplex al conectarse a una PABX o a la PSTN, todo esto con el fin de permitir la convergencia de tecnologías y borrar los límites entre sistemas sin comprometer en ningún caso la seguridad y confiabilidad del mismo.

#### 2.2.1.5 Capaz de Protocolo TETRA.

En la especificación del protocolo se utiliza una estructura de capas Figura 2.5, conforme al modelo de referencia OSI Figura 2.6. De este modo se consiguen grupos aislados de funciones que permiten su descripción como una sucesión de capas independientes, en la que cada una de ellas ofrece su servicio de comunicación a la capa superior en diferentes puntos de acceso de servicio.

**Figura 2.5. Capas TETRA**



Nº Capa	Nombre de Capa	Servicios Ofrecidos
7	Aplicación	Protocolo de soporte para los servicios de datos, voz, señalización y control
6	Presentación	
5	Sesión	
4	Transporte	
3	Red	
2	Enlace de Datos	LLC: Enlace entre móvil y base MAC:TDMA
1	Física	Parámetros RF

**Figura 2.6. Modelo de Referencia OSI**

- Capa Física

Comprende la parte de transmisión de bits y símbolos; comprendiéndose por símbolo a la unión de dos bits. La capa física tiene las siguientes funciones:

- Funciones relacionadas con el interfaz aire
  - a. Modulación/demodulación
  - b. Transmisión/Recepción
  - c. Características RF
    - Ajustes de frecuencia y canales
    - Salidas, Indicador de Potencia de Radio Señal RSSI.
  - d. Ajuste de los parámetros de radio
    - Corrección de frecuencia
    - Control de potencia
- Orientación de bits y símbolos

a. Sincronización de símbolo.- secuencia de formación específica, localización dentro de la ráfaga, secuencia de aparición de símbolos.

o Construcción de ráfaga

a. Recepción/envío de datos desde y hacia la subcapa MAC, debido a que la capa física es capaz de determinar el principio y final de la ráfaga, en la emisión, ubica el bloque MAC dentro de la ráfaga física y adiciona información específica en el lugar correcto. En recepción se extrae esta información específica de la ráfaga y se procede a la reconstrucción del bloque MAC.

b. Bandera de slot codificación/decodificación

c. Scrambling/de-scrambling. BS y MS combinan las tramas antes de ser enviadas. La combinación es realizada de acuerdo con la dirección de la base station. Esta combinación se la conoce con el nombre de "código de color.

• Capa Control de Acceso al Medio MAC

La capa 2 maneja conexiones lógicas y aísla a la capa física de las capas superiores.

MAC maneja el acceso a los canales de radio y administración de los recursos de transmisión, aquí se define el método de acceso TDMA y la codificación de canal. Las funciones que ejecuta esta capa son:

o Codificación de canal

- a. Interleaving/de-interleaving y reordenamiento de bits. Esto permite el esparcimiento de errores en lugar de tenerlos agrupados como es el caso de la transmisión por radio.
  - b. Codificación de canal.
    - Protección de los datos en el camino de la transmisión, para esto utiliza Corrección de errores hacia adelante FEC
    - Se utiliza Control de Redundancia Cíclica CRC en el comienzo del bloque de información, así los errores pueden ser detectados antes de una cierta cantidad.
- Control de acceso al canal de radio
- a. Sincronización de trama. Se realiza un seguimiento del número de la trama dentro de una multitrama.
  - b. Procedimiento de acceso aleatorio.
    - Control de contención a un canal físico
    - Control de flujo del enlace ascendente
  - c. Fragmentación/re-asociación
    - Divide el contenido de una Unidad de Servicio de Datos SDU en algunas Unidades de Datos de Protocolo PDUs. Por otro lado, las partes son re-asociadas en el orden original.
  - d. Multiplexación/de-multiplexación de los canales lógicos

- e. Construcción y sincronización de multitramas, cuando las tramas se alistan para formar multitramas o hipertramas.
- o Administración de recursos de radio

Exclusivo para un MS o BS. Permite control de potencia sobre los recursos de radio para ser habilitados en cualquier instante sin necesidad de la intervención de la capa 3. Las funciones que se cumplen son las siguientes:

- a. Medida de BER y BLER (Block Error Rate), en forma independiente o con el control de otras capas.
  - b. Cálculo de pérdidas en la trayectoria: Supervisión de celdas y monitoreo de celdas adyacentes.
  - c. Administración de direcciones para llamadas individuales y grupales o de broadcast.
  - d. Administración de control de potencia. (Excepto en la capa física)
  - e. Establecimiento de la trayectoria: frecuencia, timeslot y selección del código de color de acuerdo a las indicaciones de la capa 3.
  - f. Asignación de recursos de radio: La asignación del canal puede depender del modo de operación del sistema.
  - g. Almacenamiento de información de control y tráfico de voz hasta su transmisión
  - h. Aplicaciones en modo circuito
- Capa Control de Enlace Lógico LLC



LLC maneja enlaces punto a punto entre MS y BS. Usado para operaciones en el plano de control (Control Plane). Se proporcionan dos clases de servicios:

- Un enlace básico, que no necesita del establecimiento de fase;
- Un enlace avanzado para un mejor grado de servicio.

Las funciones de la capa LLC son las siguientes:

- a. Intercambio de control y/o datos de usuario
- b. Manejo del enlace lógico
- c. Planificación de la transmisión de datos
- d. Re-transmisiones
- e. Segmentación/Re-ensamblaje
- f. Medición de errores
- g. Control de flujo
- h. Acuse de recibo de datos
- i. Asignación y negociación de canales lógicos.

- Capa Entidad de Control del Enlace Móvil/Base MLE/BLE

En la capa 3 se manejan los procedimientos de red.

La capa MLE/BLE, esta aplicada al Plano de Control (c-plane), sirve de plataforma para los servicios en la capa red. Las funciones son las siguientes:

- a. Discriminación de protocolos
- b. Administración de la asociación móvil-base
- c. Administración de Identidad
- d. Selección de la calidad de servicio QoS
- e. Movilidad dentro del área registrada (RA)

- Administración de Movilidad MM

Las funciones que realiza MM son las siguientes:

- a. Selección de la localización del Área (LA)
- b. Registro
- c. Autenticación
- d. Conexiones de usuario
- e. Selección de la red

- Entidad de Control en Modo Circuito CMCE

A su vez CMCE es subdividida en tres sub-entidades SDS, CC, y Control de Servicios Suplementarios.

- *Servicio de Datos Cortos SDS*

SDS maneja mensajes de datos no orientados a conexión, con las siguientes capacidades:

- Minimiza el número de transmisiones requeridas para el envío de datos cortos, como mensajes de señalización.
- Direcciones fuente y destino asociadas a mensajes de datos cortos
- Codificación eficiente al enviar mensajes

- *Control de Llamada CC*

CC maneja llamadas en modo circuito con las siguientes funciones:

- Establecimiento, mantenimiento y terminación de llamadas de servicio básico.
- Identidad de llamada

- *Servicios de Control Suplementarios*

Cumple con las siguientes funciones:

- Activación/desactivación
- Registro
- Invocación y operación
- cancelación

- Protocolo de Manejo de Datos PDP

PDP Maneja el protocolo de Internet IP v4 e IPv6.

#### 2.2.1.6 GATEWAYS (Pasarelas)

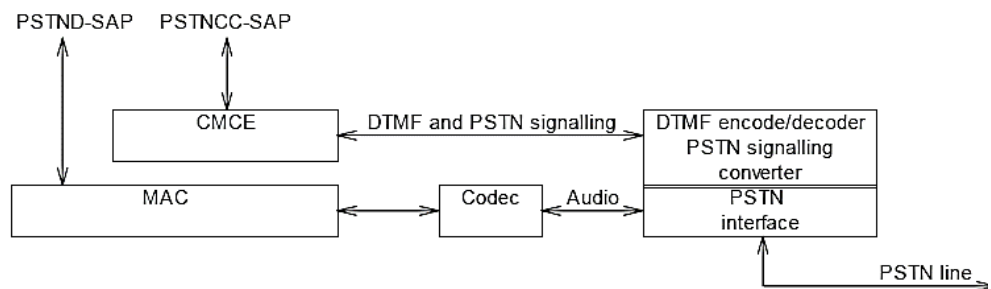
Un gateway o pasarela permite establecer comunicación entre usuarios de redes TETRA en este caso con usuarios de otras redes que no sean TETRA.

El estándar TETRA considera 3 tipos de gateway para establecer conexión con las 3 redes consideradas de mayor importancia, la red telefónica pública conmutada (PSTN), la red digital de servicios integrados (ISDN) y una red de datos empaquetados, en el Release 1 se desarrolló para la red X.25, luego se desarrollaría el protocolo PDP para soportar redes con arquitectura TCP/IP.

- GATEWAY PSTN

El gateway PSTN permite establecer llamadas entre usuarios PSTN y usuarios TETRA, este quizás es el establecimiento más complicado ya que se necesita integrar la

PSTN que tiene información y señalización analógica con la red TETRA en la cual tanto la información como la señalización son de naturaleza digital. La Fig. 27 muestra el esquema del stack de protocolos del gateway PSTN.



**FIGURA 2.7** Configuración del Gateway PSTN TETRA

Fuente: (ETSI T., ETS 300 392 - 4 - 1)

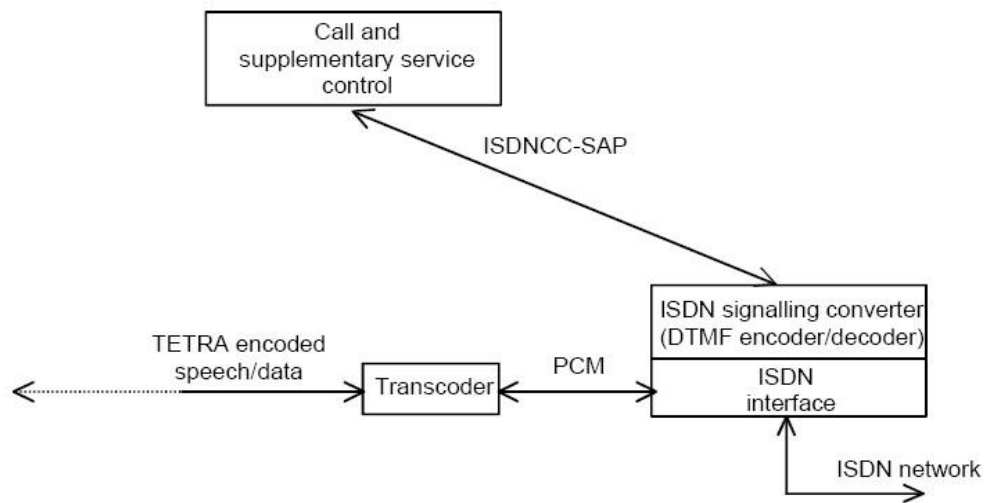
Donde se puede apreciar los SAPs PSTND (Datos PSTN) y PSTNCC (Control de llamada), por el uno se intercambiara información (voz) y por el otro se realizara la conversión de la señalización TETRA a PSTN (utilizando DTMF (Multifrecuencia de Tono Dual)) y viceversa.

En el caso de la voz se necesita de un transcoder que realice la conversión de un vocoder ACELP de baja velocidad (4.567 Kbps) utilizado en TETRA a un codificador de relativamente más alta velocidad (32 kbps utilizando ADPCM o 64 kbps utilizando PCM).

- GATEWAY ISDN

El gateway ISDN permite tanto que un usuario ISDN establezca una llamada con un usuario TETRA como a la inversa, que un usuario TETRA establezca una llamada con un usuario ISDN.

Para la señalización se ha establecido que la red ISDN se comunicara con la infraestructura SwMI de acuerdo con los procedimientos de control de llamada (CC), mientras que la red TETRA se comunicara con la red ISDN de acuerdo con los procedimientos de control de llamada DSS1 definidos en el estándar EN 300 403 – 1. La Fig. 2.8 muestra el stack de protocolos del gateway ISDN



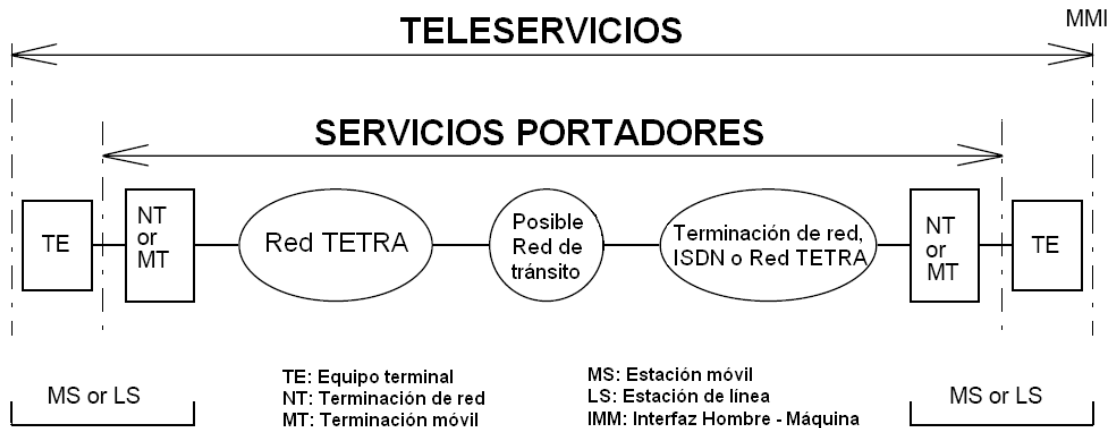
**Figura 2.8** Configuración del gateway ISDN TETRA

Fuente: (ETSI T. , ETS 300 392 - 4 - 1, European Standard)

El gateway ISDN será aplicable tanto en comunicaciones punto – punto, como punto – multipunto en modo circuito y teleservicios donde se curse voz y datos.

### 2.2.1.7 Servicios

Los sistemas TETRA definen dos tipos de servicios básicos que pueden ser prestados dentro de la red, los llamados Teleservicios y Servicios Portadores, además se define los servicios complementarios a los básicos ya mencionados. La Fig. 2.9 muestra la clasificación de servicios en los sistemas TETRA.



**Figura 2.9** Clasificación de los servicios en los sistemas TETRA.

Fuente: (ETSI E. T., 1997)

- Teleservicios

A este tipo de servicio el usuario puede acceder a través de la interfaz MMI (Interfaz Hombre – Máquina). Una llamada individual o de grupo son ejemplos de teleservicios debido a que se utiliza un teclado para hacer la llamada. Los teleservicios proporcionan capacidad completa incluyendo funciones adicionales de los terminales. Estas características están asociadas a las capas más altas (capas de la 4 a la 7) de acuerdo al modelo de referencia OSI (del inglés Open Systems Interconnected). Los teleservicios proporcionados por sistemas TETRA son los siguientes:

- **Llamada individual.** Comparable al típico caso de la telefonía pública donde un usuario se conecta a otro mediante una llamada, el receptor puede o no pertenecer a la misma red.
- **Llamada Grupal.** La conexión se realiza entre un usuario de la red, con otros usuarios que pertenecen a un grupo. Éste grupo de usuarios puede formarse dinámicamente. Adicionalmente se puede configurar la llamada en grupo para que cada usuario confirme la recepción de dicha llamada.

- **Llamada de difusión.** Este tipo de llamadas se realizan desde el centro de control con el fin de brindar información a los usuarios de la red. No se necesita una confirmación por parte del usuario.
  - **Llamada de emergencia.** Se trata de una llamada con un nivel de prioridad alto, con el fin de que la comunicación se efectúe de la manera más pronta.
  - **Operación en modo directo DMO.** De esta forma se pueden conectar dos usuarios en modo half-duplex, en forma directa sin necesidad de utilizar la infraestructura de la red.
  - **Canal abierto.** Similar al servicio de un canal analógico de radio de dos vías en donde el usuario puede participar y escuchar libremente.
  - **Inclusión de llamada.** Permite incluir a un participante, en una conversación grupal que ha sido establecida previamente.
- **Servicios Portadores**

En los servicios portadores existe capacidad de comunicación entre las interfaces de los terminales de red pero excluye las funciones adicionales de los equipos terminales. Estas características están asociadas a las capas más bajas (capas de la 1 a la 3) de acuerdo al modelo de referencia OSI. Los servicios portadores soportados por los sistemas TETRA son los siguientes:

- **Transmisión del estado de usuario.** Es utilizado para utilizar mensajes cortos predefinidos tales como: “recibido”, “petición de trabajo”, “regresar a base”, etc.
- **Servicios de Datos Cortos.** Brinda mensajería de datos cortos entre usuarios de la red, similar a los mensajes SMS en redes celulares.

- Servicio de Datos sobre Circuitos Conmutados. Utilizado en modo no protegido es decir a una velocidad de 7.2 Kbps por ranura de tiempo.
- Servicio de Datos sobre Paquetes conmutados. Basado en el protocolo TCP/IP o X.25 dependiendo del tipo de aplicación. La velocidad máxima es 28,8 Kbps.
- Servicios Suplementarios

Se denominan servicios suplementarios a aquellos que modifican o complementan a los servicios básicos, sean estos teleservicios o portadores. Los servicios complementarios que son soportados en los sistemas TETRA son los siguientes:

<i>Servicios Suplementarios Esenciales</i>		
Llamada autorizada por despachador	Las llamadas pueden ser procesadas solo con la autorización del despachador.	
Acceso Prioritario	Permite el acceso al usuario en el caso de que exista congestión.	
Prioridad de llamada	Las llamadas son asignadas por un valor de prioridad, las prioridades altas tienen mayor peso a la hora del acceso.	
Acceso tardío	Para unirse a un grupo que tiene una llamada en proceso.	
Escucha Discreta	Para interceptar la conexión en curso, sin alertar a las partes involucradas	
Ambiente de escucha	Para redirigir una transmisión de una terminal.	
Número de grupo dinámico	Asignación	Para la creación, modificación y eliminación dinámica de grupos de usuarios
	Identificación de grupos de llamadas	Para conocer la identidad de quien llama durante llamadas grupales



	Prioridad para llamadas preventivas	Para permitir la interrupción de una llamada con un menor nivel de prioridad.
--	-------------------------------------	---

<i>Servicios Suplementarios Opcionales</i>	
Selección de área	El usuario puede elegir las áreas en las que la llamada puede ser procesada. Si el usuario se encuentra fuera de estas áreas, la llamada será no exitosa.
Identificador de llamada	Permite a los usuarios desplegar en la pantalla de su terminal el número de quien realiza la llamada.
Desvío de llamada incondicional	Para desviar una llamada a un número definido por el usuario. De manera permanente
Desvío de llamada en caso de ocupación	Desvía la llamada cuando el usuario al que se realiza la llamada se encuentra ocupado
Desvío de llamada en caso de no contestación	Se desvía la llamada a un nuevo terminal en el caso de que la llamada original no sea atendida
Lista de búsqueda de llamada	Una llamada es dirigida a la primera dirección de una lista de llamadas
Abreviación de llamada	El usuario puede programar su terminal para que una dirección marcada sea grabada y luego marcar con una determinada tecla
Llamada en espera	Sirve para alertar al usuario que una nueva llamada esta llegando, esta nueva llamada puede ser atendida o rechazada.
Retención de llamada	Para la interrupción y posterior recuperación de una llamada
Completar una llamada cuando el usuario esta ocupado	La red se encarga de retardar la llamada hasta que el usuario en recepción, tenga la capacidad de contestar

### **2.2.2 VoIP**

VoIP es un estándar de la ITU (Internacional Telecommunications Union), creado en 1996 con el objeto de proporcionar una base desde la cual los desarrolladores puedan evolucionar en conjunto. El concepto de Telefonía IP es sinónimo de VoIP, es la implementación y utilización de VoIP. Es la posibilidad de transportar conversaciones telefónicas en paquetes IP. Cuando hablamos de "VoIP", nos referimos a "la telefonía en Internet" en el sentido más amplio de la expresión. El término VoIP no se refiere a ninguno de los mecanismos concretos que existen para llevar las señales de voz de un sitio a otro en la red. Existen docena de tecnologías que permiten hablar por la red. 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. Como se había mencionado anteriormente

### **2.2.3 Telefonía IP.**

La telefonía IP también llamada Voz sobre IP se puede definir como la transmisión de paquetes de voz utilizando redes de datos, la comunicación se realiza por medio del protocolo IP (Internet Protocol), permitiendo establecer llamadas de voz y fax sobre conexiones IP (Redes de Datos Corporativos, Intranets, Internet, etc.), obteniendo de esta manera una reducción de costos considerables en telefonía.

Existen varias definiciones, todas concluyen en un punto importante: Envío de voz comprimida y digitalizada en paquetes de datos y sobre protocolo de Internet (IP), utilizando redes de datos aprovechando el ancho de banda que ofrece y el cableado, ahorrando costos importantes para las empresas. Algunas de estas definiciones son:

- Voz sobre IP se puede definir como una aplicación de telefonía que puede ser habilitada a través de una red de datos de conmutación de paquetes vía protocolo IP (Internet Protocol). La ventaja real de ésta es la transmisión de voz como datos, ya que se mejora la eficiencia del ancho de banda para transmisión de voz en tiempo real en un factor de 10.
- VoIP es una tecnología que tiene todos los elementos para su rápido desarrollo. Como muestra se puede ver que compañías como Cisco, la han incorporado a su catálogo de productos, los teléfonos IP están ya disponibles y los principales operadores mundiales, así como “Telefónica” (operadora española de servicios de telecomunicaciones), están promoviendo activamente el servicio IP a las empresas, ofreciendo calidad de voz a través del mismo. Por otro lado se tiene ya un estándar que garantiza interoperabilidad entre los distintos fabricantes. La conclusión parece lógica: hay que estudiar cómo poder implantar VoIP en nuestra empresa.
- Se define la telefonía IP como el uso de paquetes IP para tráfico de voz full- duplex. Estos paquetes son transmitidos a través de internet o de redes IP privadas. El componente clave de la tecnología en telefonía IP son los equipos que convierten la señal de voz analógica en paquetes IP. Estos equipos pueden ser tarjetas específicas para PC, software específico o servidores-pasarela de voz. Estos equipos consiguen una calidad comparable a la telefonía móvil analógica a 5 Kbps. a partir de algoritmos de compresión que explotan las redundancias, pausas y silencios del habla.
- La telefonía IP es una tecnología que permite el transporte de voz sobre redes IP, produciendo un efectivo ahorro en el gasto que incurren las corporaciones para sus llamadas de larga distancia nacional e internacional. Mediante la instalación de Gateway y paquetes de software en dependencias estratégicas de la corporación, es posible obtener beneficios económicos

tangibles a corto plazo al sustituir minutos de larga distancia convencional por minutos de voz sobre IP a un costo menor.

El Protocolo Internet en un principio se utilizó para el envío de datos, actualmente debido al creciente avance tecnológico, es posible enviar también voz digitalizada y comprimida en paquetes de datos, los cuales pueden ser enviados a través de Frame Relay, ATM, Satélite, etc. Una vez que estos paquetes llegan a su destino son nuevamente reconvertidos en voz.

#### 2.2.3.1 Como funciona Telefonía IP

La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien provisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET.

Las arquitecturas interoperables de voz sobre IP se basan en la especificación H.323, en el protocolo SIP o el protocolo IAX. La especificación H.323 define gateways (interfaces de telefonía con la red) y gatekeepers o servidores IP (componentes de conmutación interoficinas) y sugiere la manera de establecer, enrutar y terminar llamadas telefónicas a través de Internet, mientras que en el protocolo SIP la manera de estructurar la red es más avanzada dejando atrás el protocolo que nació con la telefonía IP, este tipo de protocolo de comunicación fue desarrollado por el grupo MMUSIC (Multimedia Sesión Control) del IETF, definiendo una arquitectura de señalización y control para VoIP, estos sistemas de comunicación utilizan por otra parte el protocolo IAX (Inter-Asterisk eXchange protocol), el cual es uno de los es uno de los protocolos utilizado por Asterisk, el cual es un servidor PBX (centralita

telefónica) de código abierto, el cual es utilizado para manejar conexiones VoIP entre servidores Asterisk, entre servidores y clientes que también utilizan protocolo IAX.

Este tipo de protocolo fue desarrollado para solucionar problemas de NAT y mejorar el trunking entre sistemas basados en este protocolo (sólo se reserva el ancho de banda necesario en cada comunicación, no como con otros TDM o IP que reservan un determinado ancho de banda), en las comunicaciones basadas en IAX, la central Asterisk puede operar de dos formas diferentes: Servidor: Como Servidor, Asterisk admite registros de clientes IAX, pudiendo ser estos clientes Hardware, Software u otros Asterisk. Cliente: Como Cliente, Asterisk puede registrarse en otros Asterisk o en operadores IP que utilicen este protocolo.

#### 2.2.3.2 Características de la telefonía IP

- Es un sistema de comunicación que utiliza el protocolo IP como protocolo principal para establecer la comunicación por medio de datagramas o paquetes de información, los cuales se transmiten a través de una red de paquetes conmutados o de conmutación de paquetes.

- La Voz sobre IP es una tecnología de telefonía que puede ser habilitada a través de una red de datos, vía el protocolo Internet donde la ventaja real de esta tecnología es la transmisión de voz de forma gratuita por lo que la información viaja en forma de datos

- La telefonía de voz de IP es una tecnología de aplicación inmediata de este sistema de comunicación, la cual permite hacer llamadas ordinarias desde PCS, Gateway, teléfonos IP, teléfonos ordinarios en general cualquier sistema de comunicación

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.

- Proporciona el enlace a la red telefónica tradicional.

- La telefonía IP utiliza diferentes tipos de protocolos para poder llevar o transmitir la información entre los cuales se encuentran:

- Protocolo SIP
- Protocolo H.323
- Protocolo IAX
- Protocolo MGCP

- Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:

- Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.
- Es independiente del hardware utilizado.
- Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

- Permite llevar un control de llamadas con resultados al segundo.

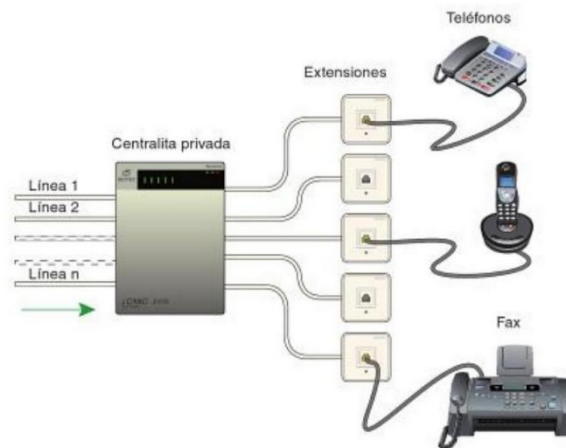
- Proporciona el enlace a la red telefónica tradicional por medio de gateway o pasarelas de comunicación

- Es independiente del hardware o sistema operativo utilizado.

#### 2.2.3.3 Centralitas privadas analógicas (RTB)

En una centralita analógica, cada extensión dispone de una línea física formada por el cable y la roseta terminal.

La conexión de cable en la centralita, tanto para las extensiones como para las líneas de entrada, se realiza, según el modelo, por conectores RJ-11 de o por bornes de inserción.



#### Ejemplo de conexión de una centralita analógica

#### 2.2.3.4 CENTRALITAS PRIVADAS DIGITALES (RDSI)

La tecnología digital está jugando un papel importante en el auge de las centralitas privadas. La centralita privada existente desde hace años, fue desarrollada para conmutar llamadas telefónicas dentro de edificios de oficinas. Las primeras centralitas privadas empleaban los métodos paso a paso o de barras cruzadas para conmutar las llamadas. Actualmente, las modernas centralitas privadas están controladas por ordenador, lo que permite que realicen multitud de funciones incluyendo digitalización de la voz y conmutación digital.

La centralita privada digital está reemplazando a la analógica, ya que es más barata, facilita el mantenimiento y realiza la conmutación de dispositivos digitales (terminales, procesadores) con mayor

eficacia. Aunque los principales proveedores continúan suministrando centralitas privadas analógicas (tal como la Dimensión de AT&T), este hecho tiende a cambiar.

La centralita privada digital emplea variantes de la modulación por impulsos codificados (MIC), para convertir señales vocales para conmutación digital. Uno de los métodos más empleados es la modulación delta, una variación del MIC.

Las nuevas centralitas privadas ofrecen las siguientes posibilidades:

- Encaminamiento de llamadas: Encaminamiento de una llamada hacia otro teléfono existente en la oficina.
- Mantenimiento automático de llamada: Cuando una llamada encuentra la extensión ocupada, se mantiene automáticamente dicha llamada hasta que la extensión quede libre.
- Llamadas de grupo: Llamadas que conectan a más de dos personas.
- Llamada rápida: Empleando un número abreviado.
- Llamada automática: Informa a la llamada que llega del estado de la conexión.
- Llamada de ruptura: Permite a ciertas estaciones interrumpir una llamada.
- Operaciones satélites: Da servicio a personas que se encuentran en puntos muy alejados.

#### 2.2.3.5 Ventajas y Desventajas de la comunicación de voz sobre IP

- Ventajas



- La ventaja más importante de la telefonía IP es el costo, una llamada mediante telefonía voz IP es en la mayoría de los casos mucho más barata que su equivalente en telefonía convencional. Esto es básicamente debido a que se utiliza la misma red para la transmisión de datos y voz, la telefonía convencional tiene costos fijos que la telefonía IP no tiene, de ahí que esta es más barata. Usualmente para una llamada entre dos teléfonos IP la llamada es gratuita, cuando se realiza una llamada de un teléfono IP a un teléfono convencional el costo corre a cargo del teléfono IP.
- Integración sobre su Intranet de la voz como un servicio más de la red, tal como otros servicios informáticos.
- Las redes IP son la red estándar universal para la Internet, Intranets y extranets.
- Estándares efectivos (H.323 y SIP)
- Interoperabilidad de diversos proveedores
- Uso de las redes de datos existentes
- Independencia de tecnologías de transporte (capa 2), asegurando la inversión.
- Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay)
- No paga SLM5 ni Larga Distancia en sus llamadas sobre IP.
- Bajos costos de operación
- Disminución de las altas facturas telefónicas
- Con VoIP uno puede realizar una llamada desde cualquier lado que exista conectividad a Internet. Dado que los teléfonos IP transmiten su información a través de Internet estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión. Esto es una ventaja para las personas que

suelen viajar mucho, estas personas pueden llevar su teléfono consigo siempre teniendo acceso a su servicio de telefonía IP.

○ La mayoría de los proveedores de VOIP entregan características por las cuales las operadoras de telefonía convencional cobran tarifas aparte. Un servicio de VOIP incluye:

- Identificación de llamadas.
- Servicio de llamadas en espera
- Servicio de transferencia de llamadas
- Repetir llamada
- Devolver llamada
- Llamada de 3 líneas (three-way calling).

○ En base al servicio de identificación de llamadas existen también características avanzadas referentes a la manera en que las llamadas de un teléfono en particular son respondidas. Por ejemplo, con una misma llamada en Telefonía IP puedes:

- Desviar la llamada a un teléfono particular
- Enviar la llamada directamente al correo de voz
- Dar a la llamada una señal de ocupado.
- Mostrar un mensaje de fuera de servicio

- Desventajas

○ La telefonía de voz sobre IP requiere de una conexión eléctrica, En caso de un corte eléctrico que a diferencia de los teléfonos VoIP los teléfonos de la telefonía convencional siguen funcionando (excepto que se trate de teléfonos inalámbricos). Esto es así porque el cable telefónico es todo lo que un teléfono convencional necesita para funcionar.

○ Dado que VOIP utiliza una conexión de red la calidad del servicio se ve afectado por la calidad de esta línea de datos, esto quiere decir que la calidad de una

conexión VoIP se puede ver afectada por problemas como la alta latencia (tiempo de respuesta) o la pérdida de paquetes. Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas. Es indispensable para establecer conversaciones VOIP satisfactorias contar con una cierta estabilidad y calidad en la línea de datos.

- VOIP es susceptible a virus gusanos y hacking, a pesar de que esto es muy raro y los desarrolladores de VOIP están trabajando en la encriptación para solucionar este tipo de problemas.

- En los casos en que se utilice un softphone la calidad de la comunicación VOIP se puede ver afectada por la PC, digamos que estamos realizando una llamada y en un determinado momento se abre un programa que utiliza el 100% de la capacidad de nuestro CPU, en este caso crítico la calidad de la comunicación VOIP se puede ver comprometida porque el procesador se encuentra trabajando a tiempo completo, por eso, es recomendable utilizar un buen equipo junto con su configuración voz IP.

- De todos modos, con la evolución tecnológica la telefonía IP va a superar estos problemas, y se estima que reemplace a la telefonía convencional en el corto plazo.

#### **2.2.4 Protocolo SIP**

El protocolo SIP (Protocolo de Inicio de Sesión) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero del 1996 en la RFC 2543, ahora obsoleta con la publicación de la nueva versión RFC 3261 que se publicó en junio del 2002.

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.) SIP fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales (salvo el rutado de los mensajes SIP).

El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales. SIP soporta funcionalidades para el establecimiento y finalización de las sesiones multimedia: localización, disponibilidad, utilización de recursos, y características de negociación.

#### 2.2.4.1 Componentes SIP

Para implementar estas funcionalidades, existen varios componentes distintos en SIP. Existen dos elementos fundamentales, los agentes de usuario (UA) y los servidores:

- User Agent (UA)

Consisten en dos partes distintas, el User Agent Client (UAC) y el User Agent Server (UAS). Un UAC es una entidad lógica que genera peticiones SIP y recibe respuestas a esas peticiones. Un UAS es una entidad lógica que genera respuestas a las peticiones SIP. Ambos se encuentran en todos los agentes de usuario, así permiten la comunicación entre diferentes agentes de usuario mediante comunicaciones de tipo cliente-servidor.

- Servidores SIP

Los servidores SIP pueden ser de tres tipos:

- Proxy Server
  - Registrar Server
  - Redirect Server
- Proxy Server

Retransmiten solicitudes y deciden a qué otro servidor debe remitir, alterando los campos de la solicitud en caso necesario. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios. Este servidor tiene una funcionalidad semejante a la de un Proxy HTTP que tiene una tarea de encaminar las peticiones que recibe de otras entidades más próximas al destinatario. Existen dos tipos de Proxy Servers: Statefull Proxy y Stateless Proxy.

- Statefull Proxy; Mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias (forking), con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada.
  - Stateless Proxy; No mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes.
- Registrar Server

Es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización

y traducción de direcciones en el dominio que controla.

- Redirect Server

Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor. La división de estos servidores es conceptual y puede ser por motivos de escalabilidad y rendimiento, se puede decir que cualquiera de ellos puede estar físicamente en una única máquina.

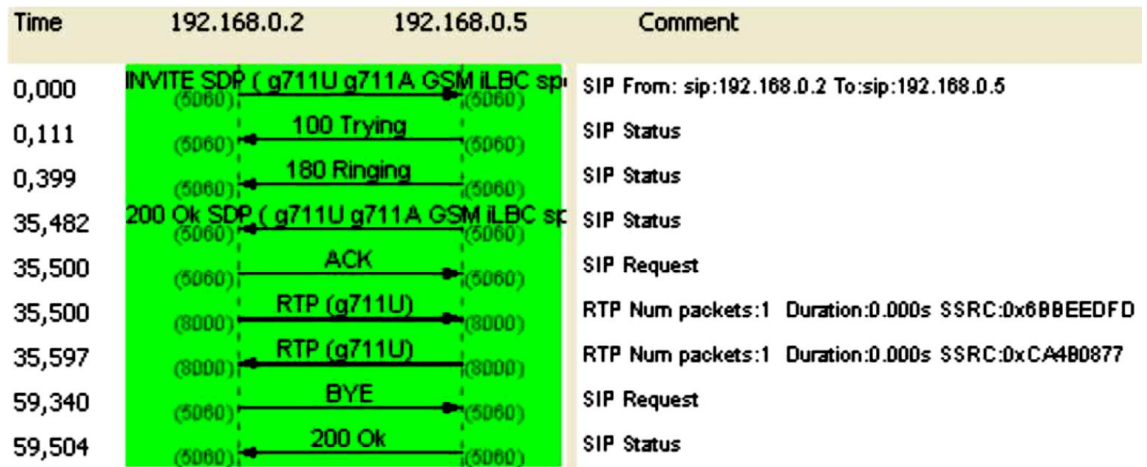
#### 2.2.4.2 Análisis del funcionamiento de SIP

SIP es un protocolo textual que usa una semántica semejante a la del protocolo HTTP. En la Fig. 2.10 se muestra como es el proceso que realizan dos terminales para establecer una comunicación SIP, los UAC realizan las peticiones y los UAS



**Figura 2.10. Peticiones y Respuestas en una llamada SIP**

SIP define la comunicación a través de dos tipos de mensajes. Las solicitudes (métodos) y las respuestas (códigos de estado) emplean el formato de mensaje genérico establecido en el RFC 2822, que consiste en una línea inicial seguida de un o más campos de cabecera (headers), una línea vacía que indica el final de las



cabeceras, y por último, el cuerpo del mensaje que es opcional.

Figura 2.11. Intercambio de mensajes en una llamada SIP

#### 2.2.4.3 Métodos SIP definidos en el RFC

SIP maneja dos tipos de métodos:

- Peticiones iniciadas por los clientes.
- Respuestas devueltas por los servidores.

Cuando un usuario cliente desea iniciar una sesión (por ejemplo, audio, vídeo, un juego), formula una petición INVITE. La petición INVITE pide establecer una sesión a un servidor. Esta petición puede ser reenviada por los SIP Proxyes, llegando eventualmente a unos o más SIP UAS que puedan potencialmente aceptar la invitación. Estos UASs necesitarán con frecuencia preguntar al usuario si acepta la invitación. Luego, estos UASs pueden aceptar la invitación (la sesión debe ser establecida) enviando una respuesta 2xx.

Si la invitación no se acepta, se envía una respuesta 3xx, un 4xx, un 5xx o 6xx, dependiendo de la razón del rechazo. Antes de enviar una respuesta final, el UAS puede también enviar respuestas provisionales (1xx) para avisar al UAC del progreso de contacto con al usuario llamado.

Los principales métodos son:

- Método SIP ACK

SIP implementa una comunicación en tres pasos:

- El que llama envía un INVITE
- El que recibe la llamada le envía una 200 OK para aceptar la llamada
- El que llama envía un ACK para confirmar el 200 OK y establecer la llamada, terminando así el proceso.

A continuación se muestra un ejemplo de una llamada real, en donde se puede apreciar la participación del método ACK.

02:28:29.0

SENDING TO: 72.55.140.84:5060.

ACK sip:00573012117233@72.55.140.84 SIP/2.0

To: <sip:00573012117233@72.55.140.84>;tag=as02cf0d4f

From: 5235113114<sip:5235113114@72.55.140.84>;tag=cf34c021

Via: SIP/2.0/UDP 192.168.0.137:7226;branch=z9hG4bKd87543- 234560215-1--d87543-;rport

Call-ID: 2368ac5f355f0654 CSeq: 2 ACK

Content-Length: 0



- Método SIP BYE

Se utiliza la petición BYE para terminar una sesión específica. En este caso, la sesión específica es la que establecida con el par UA, User Agent, (Agente Usuario) en el otro lado del diálogo. Cuando un BYE se recibe en un diálogo, cualquier sesión asociada a ese diálogo debe terminar. El UA del que llama puede enviar un BYE para los diálogos confirmados o tempranos, y el UA del llamado puede enviar un BYE en diálogos confirmados, pero no debe enviar un BYE en diálogos tempranos.

- Método SIP CANCEL

La petición CANCEL, como el nombre implica, se utiliza para cancelar una petición anterior enviada por un cliente. Específicamente, pide al UAS que deje de procesar la petición y que genere una respuesta de error a esa petición. El CANCEL no tiene ningún efecto sobre peticiones a las cuales un UAS ha dado ya una respuesta final.

Debido a esto, es más útil cancelar las peticiones las cuales puede llevar a un servidor un tiempo largo para responder. Por esta razón, el CANCEL es lo mejor para las peticiones INVITE, que pueden tomar un tiempo largo para generar una respuesta. En ese caso, un UAS que recibe un pedido de CANCEL a una INVITACIÓN pero todavía no ha enviado una respuesta final, pararía de hacer "ring", y después respondería el INVITE con una respuesta de error específica

14:28:29.1

RECEIVING FROM: 72.55.140.84:5060

SIP/2.0 200 OK

Via: SIP/2.0/UDP 192.168.0.137:7226;branch=z9hG4bKd87543-

234560215-1--d87543-

;received=200.106.178.61;rport=64343 From:

5235113114<sip:5235113114@72.55.140.84>;tag=cf34c021

To:<sip:00573012117233@72.55.140.84>;tag=as02cf0d4f

Call-ID: 2368ac5f355f0654

CSeq: 2 CANCEL

User-Agent: Cisco ATA 186 v3.1.0 atasip (040211A) Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Contact: <sip:00573012117233@72.55.140.84>Content-Length: 0

- Método SIP REGISTER

El registrarse exige enviar una petición REGISTER a un tipo especial de UAS conocido como Registrar. Un SIP Registrar Server actúa como servicio de localización para los dominios, leyendo y escribiendo los mapeos basados en el contenido de las peticiones REGISTER. Este servicio de localización entonces es consultado típicamente por un Proxy Server que sean responsable de los pedidos de enrutamiento para ese dominio. A continuación un ejemplo real, en donde la cuenta 5235113114 intenta registrarse con el Proxy SIP 72.55.140.82:

RECEIVING FROM: 72.55.140.84:5060

SIP/2.0 100 Trying

Via: SIP/2.0/UDP 192.168.0.137:7226;branch=z9hG4bKd87543-

1055408024-1--d87543-

;received=200.106.178.61;rport=64343 From:

5235113114<sip:5235113114@72.55.140.84>;tag=f9327832

To: 5235113114<sip:5235113114@72.55.140.84>

Call-ID: ea579d26a60f431c CSeq: 2 REGISTER

User-Agent: Cisco ATA 186 v3.1.0 atasip (040211A)

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Contact: <sip:5235113114@72.55.140.84>

Content-Length: 0

- Método SIP RE-INVITE

Esta modificación puede implicar el cambio de direcciones o puertos, sumando un media stream (flujo de datos de voz) o suprimiendo un media stream, etcétera. Esto se logra enviando una nueva petición INVITE dentro del mismo diálogo que estableció la sesión. Una petición INVITE enviada dentro de un diálogo existente se conoce como re-Invite.

Un solo re-Invite puede modificar el diálogo y los parámetros de la sesión en al mismo tiempo.

Los Re-Invite pueden causar muchas confusiones e inconvenientes si no se sabe qué sucede exactamente entre UAC/UAS en el momento en que se producen los re-Invite.

- Método SIP OPTIONS

El método OPTIONS permite a un UA preguntar a otro UA o a un Proxy Server en cuanto a sus capacidades. Esto permite que un cliente descubra información sobre los métodos soportados, los tipos de contenidos, las extensiones, los codecs, etc. sin tener que provocar el “ringing” de la otra parte. Por ejemplo, antes de

que un cliente inserte un campo de encabezado requiere en un INVITE opción que no es segura que sea soportada por el UAS destino, el cliente puede preguntar al UAS destino con un mensaje OPTIONS para ver si esta opción es devuelta en el campo del encabezado Supported.

#### 2.2.4.4 Respuestas (Códigos de estado) SIP

Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor del mismo responde con un mensaje. Este mensaje, es similar al anterior, difiriendo en la línea inicial, llamada Status-Line, que contiene la versión de SIP, el código de la respuesta (Status-Code) y una pequeña descripción (Reason-Phrase). El código de la respuesta está compuesto por tres dígitos que permiten clasificar los diferentes tipos existentes. El primer dígito define la clase de la respuesta:

1xx = respuestas informativas

- 100 Tratando
- 180 Teléfono sonando
- 181 Llamada esta siendo redireccionada
- 182 Encolada
- 183 Progreso de sesión

2xx = respuestas de éxito

- 200 OK
- 202 aceptada: Utilizada por referidos

3xx = respuestas de redirección

- 300 Múltiples opciones
- 301 Movido permanentemente
- 302 Movido temporalmente
- 305 Utiliza Proxy

- 380 Servicio alternativo

#### 2.2.4.5 Mensajes de errores

A continuación se muestran los errores que se pueden producir en los mensajes SIP de manera más detallada explicando la causa concreta del error: Como se ha indicado anteriormente corresponde con las respuestas de la clase:

- 4xx - Respuestas de fallos de solicitud
- 5xx - Respuestas de fallos de servidor.
- 6xx - Respuestas de fallos globales.

#### 2.2.4.6 Cabecera

Las cabeceras se utilizan para transportar información necesaria a las entidades SIP. A continuación, se detallan los campos:

- Vía: Indica el transporte usado para el envío e identifica la ruta del request, por ello cada proxy añade una línea a este campo.
- From: Indica la dirección del origen de la petición.
- To: Indica la dirección del destinatario de la petición.
- Call-Id: Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de una transacción.
- Cseq: Se inicia con un número aleatorio e identifica de forma secuencial cada petición.
- Contact : Contiene una (o más) dirección que puede ser usada para contactar con el usuario.

•User Agent: Contiene el cliente agente que realiza la comunicación.

Ejemplo de cabecera: A continuación se observa la cabecera obtenida de una llamada real cuando la cuenta 5235113114 registrada en el Proxy

SIP 72.55.140.84 intenta comunicarse con el destino 111.

SENDING TO: 72.55.140.84:5060

INVITE sip:111@72.55.140.84 SIP/2.0

To: <sip:111@72.55.140.84>

From:5235113114<sip:5235113114@72.55.140.84>;tag=d410e329

Via: SIP/2.0/UDP 192.168.0.137:7226;branch=z9hG4bKd87543-

372391639-1--d87543-;rport

Call-ID: b368b3165d43ce4c

CSeq: 2 INVITE

Contact: <sip:5235113114@192.168.0.137:7226>

Max-Forwards: 70

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER,

NOTIFY, MESSAGE, SUBSCRIBE, INFO

Content-Type: application/sdp

Proxy-Authorization:Digest

username="5235113114",realm="asterisk",nonce="6c9a1825",uri="sip:111@72.55.140.84",response="fc1b5bdf31d7e733411dea0d99dd2c1a",algorithm=MD5

User-Agent: eyeBeam release 3007n stamp 17816 Content-Length: 274

#### 2.2.4.7 Descripción del direccionamiento en SIP

Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres. Normalmente, el agente de

usuario no conoce la dirección IP del destinatario de la llamada, sino su e-mail.

Las entidades SIP identifican a un usuario con las SIP URI (Uniform Resource Identifiers) definido en el RFC 2396. Una SIP URI tiene un formato similar al del e-mail, consta de un usuario y un dominio delimitado por una @, como muestra los siguientes casos:

*usuario@dominio*, donde dominio es un nombre de dominio completo.

*usuario@equipo*, donde equipo es el nombre de la máquina.

*usuario@dirección\_ip*, donde dirección ip es la dirección IP del dispositivo.

*número\_teléfono@gateway*, donde el gateway permite acceder al número de teléfono a través de la red telefónica pública.

La solución de identificación de SIP, también puede ser basada en el DNS escrito en el RFC 3263, donde se describen los procedimientos DNS utilizados por los clientes para traducir una SIP URI en una dirección IP, puerta y protocolo de transporte utilizado, o por los servidores para retornar una respuesta al cliente en caso de que la petición falle.

#### 2.2.4.8 Análisis de una llamada SIP

Como lo muestra la Fig. 6 en una llamada SIP hay varias transacciones SIP. Una transacción SIP se realiza mediante un intercambio de mensajes entre un cliente y un servidor.

Consta de varias peticiones y respuestas y para agruparlas en la misma transacción está el parámetro CSeq.

Las dos primeras transacciones corresponden al registro de los usuarios. Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor Proxy, que actúa como Register, consulta si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo.

La siguiente transacción corresponde a un establecimiento de sesión. Esta sesión consiste en una petición INVITE del usuario al Proxy. Inmediatamente, el Proxy envía un TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario B envía un Ringing 180 cuando el teléfono empieza a sonar y también es reenviado por el Proxy hacia el usuario A. Por último, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).

En este momento la llamada está establecida, pasa a funcionar el protocolo de transporte RTP; Con los parámetros (puertos, direcciones, codecs, etc.) establecidos en la negociación mediante el protocolo SDP.

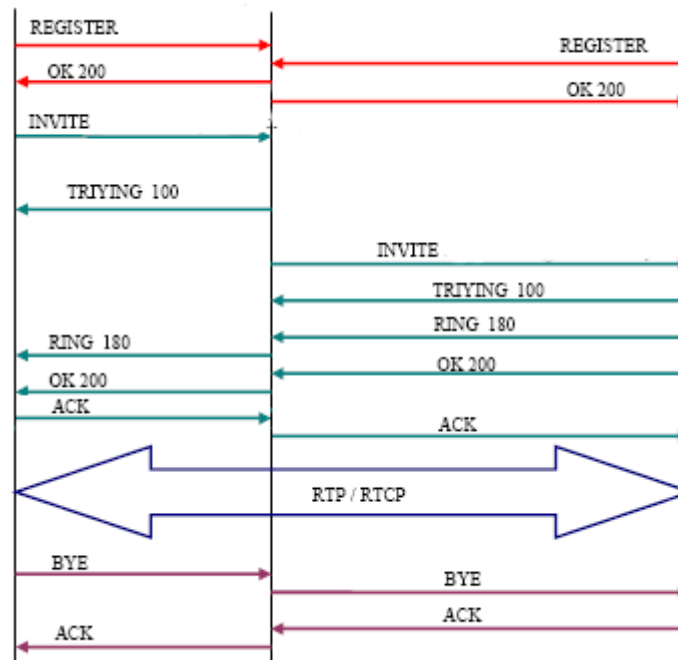
La última transacción corresponde a una finalización de sesión. Esta finalización se lleva a cabo con una única petición BYE enviada al Proxy, y Posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

Usuario A

Poxy SIP

Usuario B





**Figura 2.11 Momentos de una llamada SIP2.**

#### 2.2.4.9 Análisis del estándar SIP

Lo que concierne a características avanzadas.

- Tienes señalización multicast
- Control de la llamada de un tercero, según se describe en los borradores (Drafts) del protocolo.
- Tiene conferencia.
- Tiene pinchar para llamar.

Lo que concierne a escalabilidad.

- Número amplio de dominios, SIP soporta de manera inherente direccionamientos de áreas. Cuando muchos servidores están implicados en una llamada SIP usa un algoritmo similar a BGP que puede ser usado en una manera sin estado evitando problemas de escalabilidad. Los SIP Registrar y servidores de redirección fueron diseñados para soportar localización de usuarios.

- Gran cantidad de llamadas, SIP soporta escalabilidad n a n entre UAs y servidores. SIP necesita menos ciclos de CPU para generar mensajes de señalización. Por lo tanto, teóricamente un servidor puede manejar más transacciones. SIP ha especificado un método de balanceado de carga basado en el mecanismo de traslación DNS SRV.
- Estado de la conexión, Con estado o sin estado una llamada SIP es independiente de la existencia de una conexión en la capa de transporte, pero sin embargo la señalización de llamadas tiene que ser terminada explícitamente.
- Internacionalización, SIP usa Unicode (ISO 10646-1), codificado como UTF-8, para todas las cadenas de texto, permitiendo todos los caracteres para nombres, mensajes y parámetros. SIP provee métodos para la indicación del idioma y preferencias del idioma.
- Seguridad, SIP soporta autenticación de llamante y llamado mediante mecanismos HTTP. Autenticación criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-TTP. Claves para encriptación multimedia se ofrecen usando SDP. SSL soporta autenticación simétrica y asimétrica. SIP también define autenticación y encriptación final.
- Interoperabilidad entre versiones, En SIP, una nueva versión puede descartar características que no van a ser soportadas más. Esto consigue reducir el tamaño del código y la complejidad del protocolo, pero hace perder cierta compatibilidad entre versiones.

### **2.2.5 Asterisk**

Asterisk es una centralita software (PBX) de código abierto para controlar y gestionar comunicaciones de cualquier tipo. Como cualquier centralita PBX permite interconectar teléfonos y conectar dichos teléfonos a la red telefónica convencional (RTB - Red telefónica básica)- Su nombre viene del símbolo asterisco (\*) en inglés.

Asterisk es un programa de software libre que proporciona funcionalidades de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios.

Es un sistema de centralita IP utilizado por empresas de todos los tamaños para mejorar su comunicación, incluyendo a Google, Yahoo, IBM, e incluso el Ejército de EE.UU.

Lanzado hace 10 años y constantemente desarrollada por la comunidad open source, Asterisk se ha convertido en uno de los servidores de comunicaciones más ricos en funcionalidades, escalables y sofisticados de los disponibles en la actualidad. Asterisk se mantiene como software libre para descargar y viene con todas las funciones sin restricciones de licencia. Asterisk puede funcionar con Linux, BSD, OS X y Windows, y trabajará con la mayoría de los teléfonos compatibles SIP y softphones. Todo lo que necesitas es el conocimiento técnico y experiencia para instalarlo y configurarlo.

#### 2.2.5.1 Principales Ventajas

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: 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.

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.

Interoperabilidad 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, 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.

#### 2.2.5.2 FUNCIONALIDADES BÁSICAS Y AVANZADAS

El sistema Asterisk incorpora todas las funcionalidades que pueden esperarse en una centralita convencional y asimismo muchísimas funcionalidades avanzadas que tendrían un elevado coste en sistemas tradicionales propietarios. A continuación las más importantes:

##### 2.2.5.2.1 FUNCIONES BÁSICAS

- Transferencias (directa o consultiva): Permite transferir una llamada en curso a otra extensión. Existen dos formas:

- O Transferencia atendida: consultando al nuevo destino si quiere que le pasen la llamada,

- O Transferencia directa: pasando la llamada sin consultar al destinatario.

En versiones anteriores a la 1.8, al transferir una llamada se perdía el CLID (el número del usuario llamante). Esto no ocurre con la versión 1.8, que mantiene por tanto el CLID tras una transferencia.

- Desvíos: Permiten la transferencia automática de una llamada entrante hacia un número determinado (interno o externo) cuando se cumplen determinadas condiciones: por ejemplo si el número está ocupado, si no contesta, etc.

- Capturas (de grupo o de extensión): La captura permite coger una llamada que se está recibiendo en una extensión desde otra distinta.

  - Captura de extensión: por defecto se hace con el código \*8 + la extensión.

  - Captura de grupo: se predefinen unos determinados grupos de extensiones de modo que al marcar un código de Asterisk - por defecto el \*8 - se coge cualquier llamada que esté recibiendo el grupo en el que estamos.

- Conferencia múltiple: En función del modelo de terminal se podrá establecer una comunicación entre múltiples usuarios de la centralita.

- Llamada directa a extensión: Si además del número de cabecera disponemos de diferentes números públicos (DDIs), podremos enrutar directamente la llamada entrante a uno de estos DDIs, a una extensión de la centralita.

- Ring groups: grupos de llamadas. Una llamada entrante podrá ser dirigida directamente a un ring group, que es un grupo de extensiones que sonaran de acuerdo a una determinada

estrategia previamente establecida. Si la llamada no se descuelga no podrá ser tratada posteriormente y se perderá.

- DND (Do not disturb): Opción de no molestar, que podrá ser configurado en Asterisk mediante un código o directamente en el terminal.

#### 2.2.5.2.2 FUNCIONES AVANZADAS

- Correo Vocal (Voicemail) integrado con correo electrónico. En caso de que el usuario no pueda atender una llamada, se puede programar que se transfiera a un sistema de buzón de voz. En caso de que se deje un mensaje, se enviará un correo electrónico avisando del mismo al usuario destinatario.

- Operadora Automática (IVR): Una operadora automática o IVR es una aplicación de telefonía que permite interactuar con el usuario que realiza la llamada, de forma que éste pueda pulsar opciones previamente anunciadas y acceder de forma automática a los destinos programados.

- Música en espera con archivos WAV: Asterisk nos permite introducir categorías de música en espera basadas en archivos .wav y mp3. De este modo podremos poner diferentes melodías para ser reproducidas como música en espera.

- Colas de Llamadas (ACD): Un sistema de colas o ACD es una aplicación que distribuye las llamadas entrantes a un grupo específico de agentes de acuerdo a una determinada estrategia. Si la llamada no puede ser descolgada, no se pierde y puede ser transferida a otro destino.

- Salas de Audio-Conferencias: Una sala de audioconferencias es un sistema que permite conectar a múltiples usuarios en una misma conversación telefónica. Los usuarios

pueden acceder a la sala desde una extensión interna, o bien desde el exterior (a través de un número directo o bien a través de un IVR). Es un sistema muy útil para hacer reuniones internas (por ejemplo seguimiento de ventas) o bien con clientes o proveedores. No hay una capacidad máxima de salas por lo que podremos definir tantas como nos hagan falta (la limitación principal serán los recursos del servidor). Las salas tampoco tienen una capacidad máxima de llamadas por lo que principalmente la limitación vendrá dada por el número de líneas que la empresa disponga para salir a la PSTN.

- Gestión de llamadas entrantes según horario o fecha (Time Conditions). Con la incorporación del gestor web FreePBX en su versión 2.5 o superior, es muy sencillo definir un horario y calendario laboral que nos permita hacer un tratamiento diferenciado de las llamadas entrantes según el mismo. Por ejemplo, si estamos en horario laboral y no es festivo, la llamada se envía a la extensión 100 (de operadora). En caso contrario, se puede enviar a una locución que advierta de que son horas no laborables, o bien es un día festivo.

- Extensiones DISA: Es posible configurar opciones de post marcación para determinadas llamadas entrantes, de forma que una vez hemos comunicado con la centralita, podamos llamar a un nuevo destino de forma sencilla y automatizada.

- Callback: llamada automática de respuesta a una llamada perdida. Cuando redirigimos una llamada al módulo de Callback el sistema lo que hará será colgar y originar una llamada hacia el número que nos ha llamado, de este modo se pueden centralizar costes de llamada. La llamada saldrá siguiendo las normas de routing saliente de llamadas.

- Retrollamada: funcionalidad disponible en la versión 1.8. Si se hace una llamada a una extensión y esta no contesta (por estar ocupado o ausente), se puede activar la función Asterisk de retrollamada. En cuanto el usuario llamado cuelgue, se avisa al que activo la función de retrollamada para que este pueda llamar de nuevo a la extensión inicial.

- Informes detallados de llamadas (CDR): Detalle de llamadas realizadas/recibidas por extensión, para imputación de costes departamentales, por cliente o incluso para facturación.

- Integración CTI: Integración de la telefonía con sistemas informatizados de gestión comercial o de atención al cliente (CRM). Estos sistemas permiten por ejemplo ejecutar una llamada desde el PC o bien recibir información sobre una llamada entrante en la pantalla.

### 2.2.5.3 CAPACIDADES DE LÍNEAS Y EXTENSIONES

El sistema Asterisk es sumamente flexible y soporta todos los sistema de conectividad interna o externa tanto tradicionales (PSTN, RDSI o analógicos) como los más actuales (SIP e incluso Skype).

A continuación enumeramos los tipos de puerto disponibles y sus capacidades:

#### Líneas de enlace o Trunks

Son las que permiten conectar la centralita con la red pública de telefonía. Existen las siguientes opciones:

- Enlaces RDSI: interfaces BRI o PRI. Existen configuraciones con 2, 4, 6, 8, 10 o 12 BRI o 1, 2, 4, 8 o 16 PRI. Todos ellos se suministran con cancelación de eco por Hardware.



- Enlaces Analógicos (FXO): configuraciones para 1/2/4/8 enlaces, con cancelación eco por Hw.
- Enlaces directos GSM, vía Gateways voip-GSM. Son equipos IP que incorporan bahías para colocar las tarjetas SIM, y llevan directamente tecnología 2G/3G para conexión con las redes de operador de móvil.
- Enlaces VoIP: SIP, IAX y Skype. Para optimizar las conexiones SIP es recomendable incorporar tarjetas de transcodificación para poder comprimir las sesiones RTP. El códec que se utiliza normalmente es el G729.

#### Extensiones

Son las conexiones internas que utilizan los usuarios o terminales de nuestra compañía. Existen las siguientes opciones:

- Extensiones SIP o IAX.
- Extensiones analógicas (FXS): configuraciones de 1/2/4/8...24 extensiones para conectar teléfonos analógicos o terminales de fax.
- Extensiones inalámbricas WIFI. Con soporte de diferentes terminales.
- Extensiones inalámbricas DECT-GAP estándar. Requiere de la instalación de antenas DECT IP (nosotros utilizamos la tecnología Polycom-Kirk).

#### 2.2.5.4 TELÉFONOS IP

Teléfonos IP para su solución abierta de telefonía IP (Asterisk o OpenSER). Dichos teléfonos soportan SIP, el estándar actual de señalización voip.

<b>POLYCOM</b>			
<b>Soundpoint IP 321</b> 2 líneas Display LCD 1 port RJ45 PoE		<b>SoundPoint IP 331</b> 2 líneas Display LCD 2 port RJ45 PoE	
<b>SoundPoint IP 450</b> 2 líneas Display LCD 2 port RJ45 PoE Tecnología HD		<b>SoundPoint IP 550</b> 4 líneas Display LCD 2 port RJ45 PoE	
<b>SoundPoint IP 650</b> 6 líneas Display LCD 2 port RJ45 PoE Tecnología HD		<b>SoundPoint IP 670</b> 6 líneas Display Color LCD 2 port RJ45 PoE Tecnología HD	
<b>Consola de operadora Polycom 650 + Módulos de Expansión</b> Llamadas simultáneas Hasta 4 pantallas LCD 48 botones iluminados			
<b>POLYCOM</b>			
<b>Soundpoint IP 321</b> 2 líneas Display LCD 1 port RJ45 PoE			
<b>SoundPoint IP 450</b> 2 líneas Display LCD 2 port RJ45 PoE Tecnología HD			
<b>SoundPoint IP 650</b> 6 líneas Display LCD 2 port RJ45 PoE Tecnología HD			
<b>Consola de operadora Polycom 650 + Módulos de Expansión</b> Llamadas simultáneas Hasta 4 pantallas LCD 48 botones iluminados			
<b>SoundPoint IP 331</b> 2 líneas Display LCD 2 port RJ45 PoE			
<b>SoundPoint IP 550</b> 4 líneas Display LCD 2 port RJ45 PoE			
<b>SoundPoint IP 670</b> 6 líneas Display Color LCD 2 port RJ45 PoE Tecnología HD			

### **2.2.6 Relaciones entre SIP y ASTERISK**

Existe una mala concepción sobre cómo funciona realmente el SIP porque es común pensar que es encargado de llevar los datos multimedia, así como los mensajes de sesión conjuntamente. Parte de esta afirmación es cierta, concretamente la segunda parte, dado que este protocolo fue diseñado exclusivamente como sistema de señalización conjuntamente a otro flujo de datos multimedia a través de un protocolo simultáneo (que en Asterisk sería el protocolo RTP, Protocolo de Transporte en Tiempo Real, o Real-Time Transport Protocol). Además para "complicar" el concepto, durante la transmisión también interviene un tercer protocolo "familiar" de SIP llamado SDP (Protocolo de Descripción de Sesiones, o Session Description Protocol), redactado en el RFC 4566 y embebido dentro del protocolo SIP por lo que no consumiría más recursos (por ejemplo Puertos a nivel TCP/IP), y se encargaría de enriquecer el

mensaje entre sesiones necesario para la trasmisión eficaz entre los dispositivos.

Realmente SIP no es capaz de ofrecer un servicio por sí mismo, pero contiene los mensajes primitivos para poder implementar los servicios subyacentes sobre el mismo. Por eso, SIP curiosamente, no tiene nada que ver realmente con la telefonía en sí, solo podría considerarse un estándar cualquiera de entendimiento entre dispositivos, algo que realmente todavía no se ha asentado, ya que múltiples dispositivos, aun no siguen los estándares "impuestos" dentro de los RFC, ya que aún no ha madurado hasta la categoría de estándar IEEE.

SIP se popularizo, debido que en el momento de la implementación de servicios de telefonía IP, no existían realmente grandes competidores en este aspecto. Además la seguridad utilizando SIP no prima especialmente, debido a que la trasmisión se realiza con mensajes de texto, y para encriptar la información es fundamental recurrir a extensiones independientes que transforman los mensajes en ambos nodos.

En el año 2010 nació como RFC 5456 un verdadero competidor, IAX, pero demasiado tarde, ya que el mercado de las telecomunicaciones IP (y concretamente dispositivos y productores), ya se había asentado sobre el protocolo SIP.

## **2.3 MARCO CONCEPTUAL**

### **2.3.1 Telefonía IP y TETRA**

La telefonía Ip se viene dando en todas parte, desde pequeñas empresas hasta grandes corporaciones, es una solución factible y sostenible aun con el auge de la escalabilidad de las tecnologías, esta se

viene dando simplificando la vida de los que la usan, es mas ya no hace utilización de la parte física, con los llamados softphone, se puede tener un teléfono IP para la comunicación en cualquier momento sin necesidad del hardware de un teléfono.

El TETRA, es un estándar que viene siendo utilizado en comunicaciones críticas (de emergencia), así como también en lugares de las comunicaciones son primordiales, tanto para la operación, como para la toma de decisiones, estando las personas solicitadas en lugares poco accesibles para una comunicación celular, y en el mejor de los casos si esta se da, es con una calidad por debajo de lo necesario.

### **2.3.2 Determinación de términos básicos:**

**1) ASTERISK:** Asterisk es una completa solución de centralita IP por software. Se instala sobre cualquier plataforma de servidor con sistema operativo Linux (GNU Linux) y - con los interfaces apropiados de telefonía (para líneas analógicas o RDSI) – convierte a dicho sistema en una potente centralita telefónica. Proporciona todas las funcionalidades de las grandes centralitas propietarias (buzones de voz, IVR, etc.) y ofrece algunas posibilidades y servicios no disponibles en la mayoría de ellos (grabación de llamadas, extensiones remotas).

**2) BASE TRANSCEIVER STATION (BTS):** La función principal de una BTS es proporcionar un número de canales radio a la zona a la que da servicio. La antena es omnidireccional. Una BTS con un transceptor y con codificación "full rate" proporciona 4 canales en el enlace radio, uno de los cuales se utiliza para señalización.

**3) BASE STATION CONTROLLER (BSC):** La función primaria de una BSC es el mantenimiento de la llamada, así como la adaptación de la velocidad del enlace radio al estándar de 64 Kbit/s. utilizado por la red. Desde el momento en que el usuario es móvil, éste puede estar cambiando con más o menos frecuencia de celda; el procedimiento por el que la llamada se mantiene en estas condiciones sin que se produzcan

interrupciones importantes se conoce con el nombre de "handover". TETRA proporciona unos tiempos de conmutación mucho más bajos que otros sistemas celulares.

En TETRA, durante una llamada, la estación móvil está continuamente "escuchando" a una serie de estaciones base así como informando a la BSC de la calidad de la señal con que está trabajando. Esto permite a la BSC tomar la decisión de cuando iniciar un handover y a qué célula. La BSC controla a su vez la potencia de trabajo de la estación móvil para minimizar la interferencia producida a otros usuarios y aumentar la duración de la batería.

**4) CERAGON:** Ceragon Networks Ltd. es una compañía focalizada en el diseño y manufactura de sistemas de radio de baja, mediana y alta capacidad, principalmente en radios de alta capacidad SDH/SONET que son el negocio principal desde la concepción inicial de la compañía en 1996. Con oficinas a través del mundo, ha provisto e instalado exitosamente más de 25.000 sistemas en más de 100 países en todo el mundo, pudiendo afirmar ser una de las compañías líderes en sistemas de Mediana y Alta capacidad en el mercado.

Ceragon cuenta con una plataforma integrada por diferentes soluciones de acuerdo a las necesidades de capacidades e interfaces de cada operador.

En tal sentido, esta plataforma prevé la posibilidad de intercambiar partes de la misma para adaptarse a los cambios en las redes, que muestran una dinámica sumamente activa, producto del crecimiento de las necesidades de comunicación.

Asimismo, las unidades de RF permiten el transporte del tráfico en forma independiente de las interfaces y capacidades instaladas. En caso de ser requerido el cambio de unidades interiores o módulos de las mismas no es necesario el cambio de las unidades exteriores

Por otra parte las soluciones de Cegaron están orientadas a permitir la migración paulatina del tráfico TDM a IP, proveyendo una combinación de interfaces y capacidades sumamente flexibles, basadas en el crecimiento mediante llaves de software, eliminando al máximo posible la necesidad de agregados o cambios de hardware.

**5) DISPATCHER:** Es un PC que utiliza un software para realizar el monitoreo directo del tráfico de los usuarios como:

- Escucha de llamadas
- Cancelar las llamadas
- Ingreso personalizado a la comunicación.

**6) Estación OIHM:** Esta aplicación nos permite administrar la red como (abonados, infraestructura, etc.). Está instalada en el puesto de operación (Centro Nodal).

**7) NMS (Software de Gestión de Red):** Este software permite monitorizar en tiempo real uno o varios sistemas iPECS, con lo que es posible tener un control absoluto de cualquier central desde su oficina. El NMS está diseñado para optimizar todos los recursos de red del sistema y al mismo proporcionar alertas y avisos en tiempo real del estado y funcionamiento de cada dispositivo, permitiendo además programación y actualizaciones remotas.

Además, gracias a su intuitivo y sencillo interfaz web podrá controlar todos sus sistemas desde cualquier lugar y en cualquier momento.

**8) PUERTO 5061:** Puerto de escucha de mensajería unificada utilizado por el protocolo SIP, a diferencia del puerto 5060 este si es protegido.

**9) SERVIDOR GATEWAY:** es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para

ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

**10) SERVIDOR SIP:** Un servidor SIP es el principal componente de una centralita IP, que maneja la configuración de todas las llamadas SIP en la red. Un servidor SIP es también conocido como Proxy SIP o Registrador.

**11) SWITCH:** Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.



## **CAPITULO III**

### **PROPUESTA PARA LA IMPLEMENTACIÓN DE LA TELEFONÍA IP COMO COMPLEMENTO EN LA COMUNICACIÓN DIGITAL TETRA EN CAMPAMENTOS MINEROS**

#### **3.1 ANALISIS DEL DISEÑO DE RED**

##### **3.1.1 Análisis y Diagnóstico de la Infraestructura Actual**

Tomaremos como explicación la escena de una minera que cuenta con comunicación TETRA en la provincia de Morococha – Junín. La Figura 3.1 muestra la distribución de los site's Tetra distribuidos en forma que cubren todo el campamento minero tanto de operaciones como de oficinas administrativas, en total son 6 Site's los que cubren la necesidad de comunicación de esta empresa minera. En la figura también se muestra el NOC Principal (tuctu) y el NOC secundario (Camp Nuevo).

Los diferentes sub campamentos mineros se encuentran dentro de la línea lila como lo eh tratado de ejemplificar en la Figura 3.2, la comunicación tetra en todo este proyecto minero ya está troncalizada, y el servicio de datos (internet) está ya disponible por la misma minera de tal forma que se muestra en la Figura 3.3.

La distribución de los equipos se ha dado sobre todo la seguridad (casetas, torres de vigilancia, accesos a diferentes áreas), y el área de opciones de mina (trabajo de campo, tato en autos, maquinaria y operarios de apoyo) y uy pocas al área administrativo de oficinas, a pesar que son más de 500 unidades de radios portátiles TETRA adquiridas por la empresa minera.

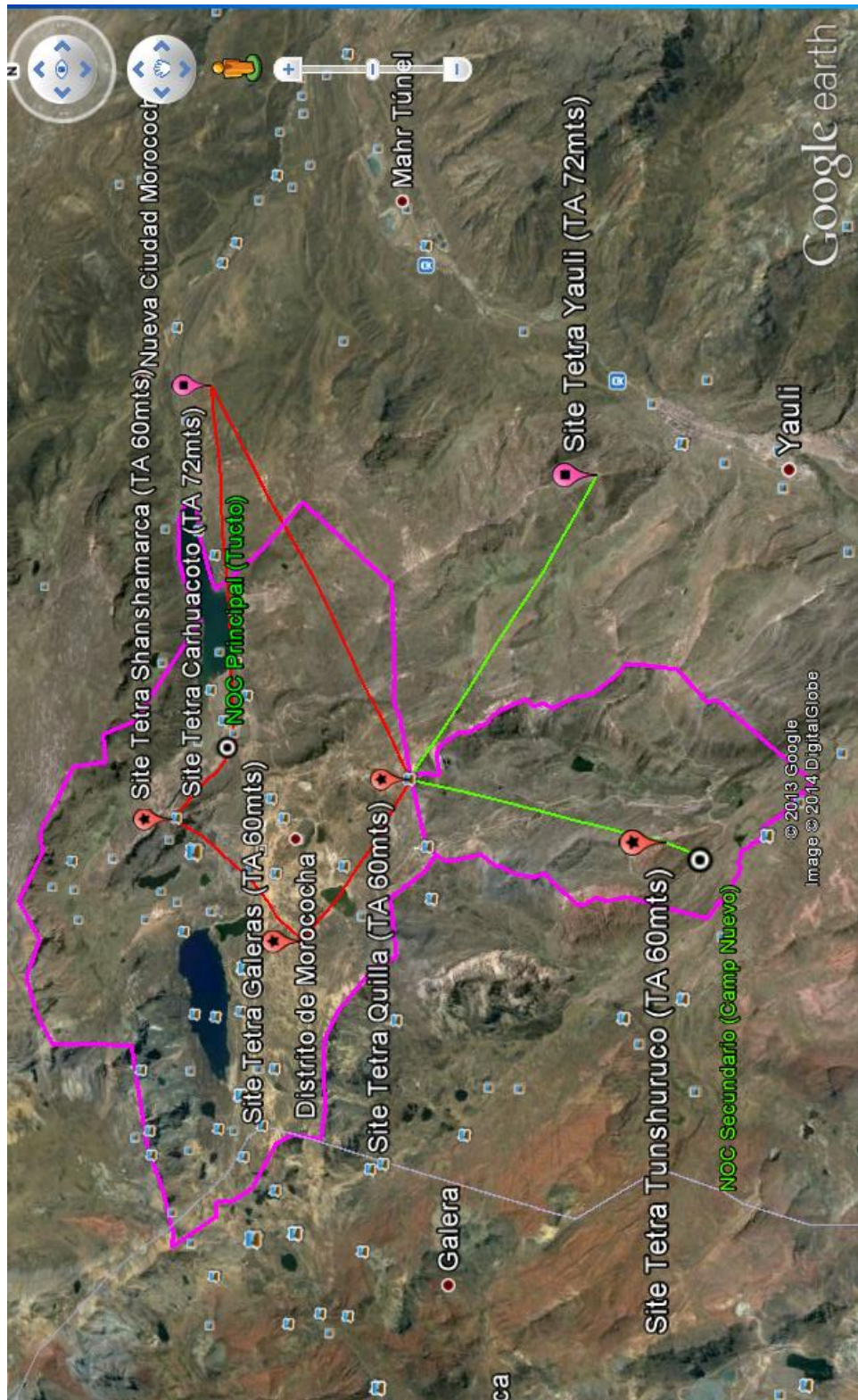


FIGURA 3.1. “distribución de Sites de la minera”.





FIGURA 3.2 “sub- campamentos”.

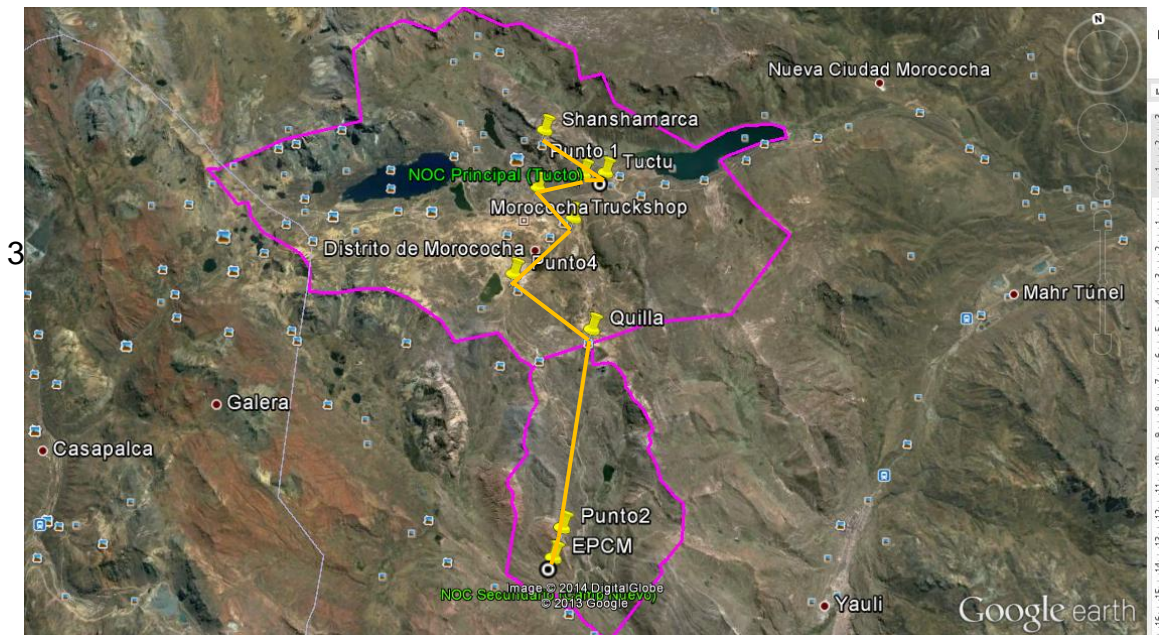


FIGURA 3.3 “servicio de Red de la minera”.

### 3.1.1.1 Detalles de la infraestructura

La infraestructura ya está dada, y será mencionada de forma general para poder ser mejor guiado el tema de instalaciones de los sistemas operativos correspondientes y de los correspondientes aplicativos. Los seis site’s tendrán una estructura igual que se describirá a líneas abajo, los otros dos puntos que tenemos que tener en cuenta son los NOC, primario y secundario, que es donde estarán

nuestros servidores por configurar para que se dé la comunicación TETRA Asterisk SIP.

#### 1) Elementos del Site.

- Civil Work (CW)
  - Soportes metálico antenas RF
  - Soportes metálico antenas Mw
- Technical Implementación (TI)
  - BTS Tetra
  - Antenas RF
  - Equipos Enlaces Mw
  - Sistemas de Alarmas
- Sistema de Power (SP)
  - Paneles solares
  - Mesa de paneles
  - Torre
  - Barras CU de RF
  - Barras CU de estructuras
  - PDP (Panel Distribución Primaria)
  - Morningstar (controlador de panel solar)
  - Sistema de Aterramiento y protección de equipos Tetra y Mw

#### **Nota:**

Se dispondrá por parte de la minera energía de 48VDC para alimentación de energía de equipos.

#### 2) Centro de Control Tetra Minera

##### 2.1 NOC Principal

El NOC Principal se ubicara en Tucto. Para lo cual se instalar 01 gabinetes indoor para el equipamiento del sistema tetra.

El Site se compone del siguiente equipamiento:

- Civil Word (CW)
  - Adecuaciones de infraestructuras existentes
  - Soportes metálicos, escalerillas, etc.
- Technical Implementation (TI)
  - Servidores (NMS, DISPATCHER, RECORDER)
  - Switch Core
  - Gateway Tetra /P25/VHF
  - Equipos Enlaces
  - Interfaces Ópticas
  - Sistema de Alarmas
- Sistema de Power (SP)
  - PDP (Panel Distribución Primaria)
  - Sistema de Energía de Respaldo Equipos (bancos 48VDC) Max 12 horas(Opcional)
  - UPS 10KW
  - Sistema de Aterramiento y protección

**Nota:**

Se dispondrá por parte de la minera energía monofásica de 220VAC estabilizada y energía 48VDC

La minera proporcionara la caseta e infraestructura (torre).

## 2.2 NOC Secundario o Redundante

El NOC Secundario se ubicara el Campamento Nuevo. Para lo cual se instalara 01 gabinetes indoor para el equipamiento del sistema tetra.

El Site se compone del siguiente equipamiento:

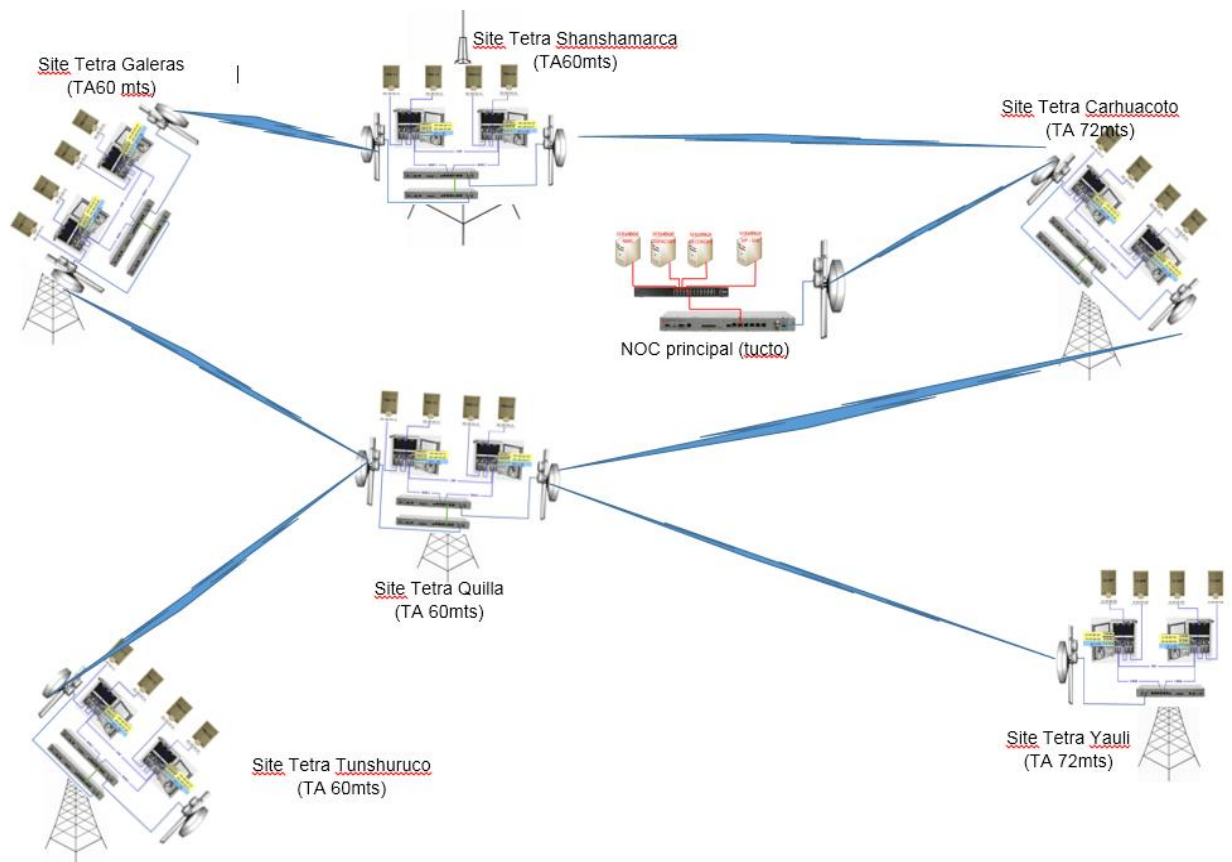
- Civil Word (CW)
  - Adecuaciones de infraestructuras existentes
  - Soportes metálicos, escalerillas, etc.
- Technical Implementation (TI)

- Servidores (NMS , FIREWALL , RECORDER)
- Equipos Enlaces Mw (Red de Transporte)
- Interfaces Ópticas
- Sistema de Alarmas
- Sistema de Power (SP)
  - PDP (Panel Distribución Primaria)
  - Sistema de Energía de Respaldo Equipos (bancos 48VDC) Max 12 horas(Opcional)
  - UPS 10KW
  - Sistema de Aterramiento y protección

**Nota:**

Se dispondrá por parte de la minera energía monofásica de 220VAC estabilizada y energía 48VDC

La minera proporcionara la caseta e infraestructura (torre).



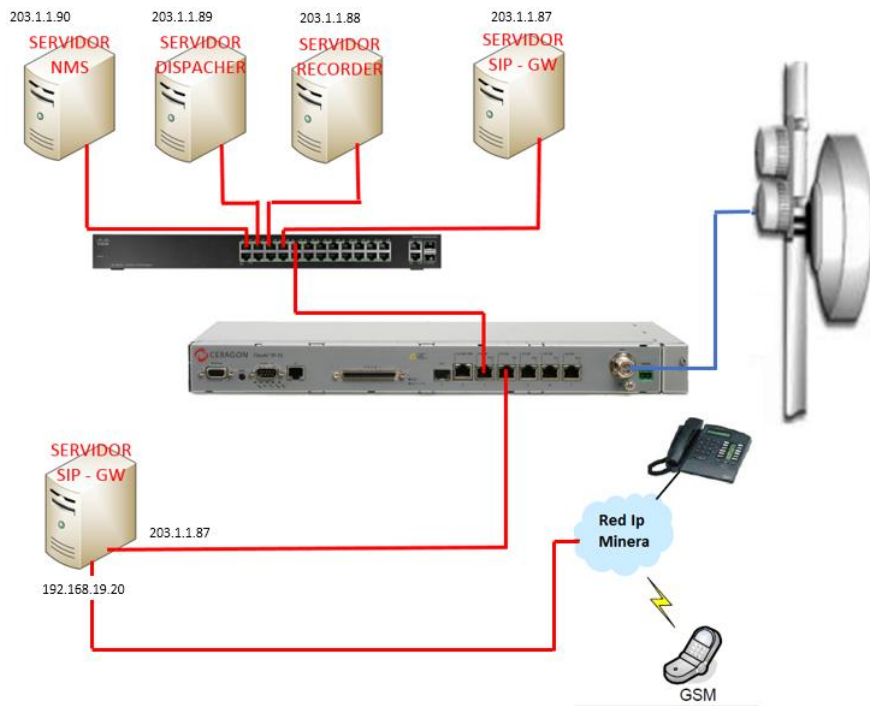
### 3.1.2 Diseño

**FIGURA 3.4** "Diseño físico de estructura TETRA - ASTERISK".

### 3.1.3 Lo que se hará

Analizando la arquitectura del sistema, toda la red física ya se encuentra dada, y disponible en la figura del diseño se ve los Site y cada uno de sus componentes pero nosotros nos centraremos en el NOC principal que es donde llegara toda nuestra data a través de los enlaces microondas pasados por un ceragon. Por lo común en el NOC principal se encuentran las interfaces hombre máquina del sistema; estamos hablando del NMS, DISPATCHER, RECODER, si bien estos interfaces son servidores dedicados, estos pueden en algún caso en especial ser virtualizados para el ahorro de espacio o recursos, en nuestro caso el análisis dándose en una empresa grande y con gran tráfico de

comunicaciones cada una de esas interfaces tendrá su servidor propio como se nota en la fig. 3.5.



**FIGURA 3.5** “diseño del NOC central”.

En la figura también podemos notar que se ha agregado al esquema común un servidor Gateway y un servidor asterisk, este último con dos tarjetas de red, una que servirá para la interfaz TETRA y la otra para la conectividad con toda la red de Ip's de la mina.

### 3.2 HABILITACIÓN DEL DISEÑO

En este punto hablaremos de la instalación del servidor SIP-Gateway (Gw) y su configuración soportados en el manual de la tecnología correspondiente.

La configuración del servidor asterisk para la vinculación entre la tecnología TETRA y la Telefonía IP (Asterisk).

La tercera comprenderá de algunas modificaciones en el Servidor NMS para el direccionamiento de búsqueda de la señalización en la base de datos.



### 3.2.1 Configuración del Servidor SIP – GW

El propósito de esta configuración es especificar las diferentes etapas de la instalación del software de la SIP GW, los servicios y la configuración de los parámetros para iniciar los diferentes servicios.

Para esto se necesitara lo siguiente:

- 1) el tipo de equipo necesario para este propósito es un servidor con lector de CD-ROM (para la instalación).y el SO. Microsoft Windows XP Service Pack 2; después de esta aplicación del software el servidor deberá de pre-configurarse con dos servicios de la tecnología TETRA, que no intervienen directamente en el la configuración para el intercambio Tetra – Asterisk; estos dos servicios son el SNMP (protocolo simple de administración de red) y el HASP (permite almacenar datos de forma transparente en dos máquinas separadas físicamente conectadas a través de la red TCP/IP) y la Instalación de componentes 2005 en tiempo de ejecución de Visual Studio (para la base de datos); teniendo esto se puedes seguir con la instalación de los paramentos específicos del servidor SIP.

#### 1.1 INSTALACIÓN DE SOFTWARE TETRA

##### 1.1.1 Ajuste de variable del entorno

Abrir el panel de sistema variable de entorno (Inicio / Configuración / Panel de control, la aplicación del sistema, fichas Avanzadas, Variables de entorno.

Agregue la siguiente ruta de acceso a la variable Path: "c: \ tetra \ palieractif \ dll".

##### 1.2 Creación de las carpetas

Seleccione la opción " C: \ Tetra \ " directorio compartido, y crear los siguientes subdirectorios:

- C:\tetra\Palieractif\DI\,
- C:\tetra\Palieractif\Exe\Outils\Pmon\,
- C:\tetra\Palieractif\Exe\SIP\FFSIP\,
- C:\tetra\Palieractif\Exe\SIP\Bcucpl\,
- C:\tetra\Palieractif\Exe\SIP\Agents\,
- C:\tetra\Palieractif\Exe\SIP\Bd\,
- C:\tetra\Palieractif\Exe\SIP\Dts\.

### 1.3 Copie los archivos del CD de instalación

#### 1.3.1 C:\tetra\Palieractif\Exe\SIP\

Buscar y copiar, en el CD de instalación, los archivos siguientes:

- FRONTAL.ini,
- CleanTrace.bat,
- CleanBDetDTS.bat,
- StartServices.bat,
- StopServices.bat.

Pegar en la ramificación creado previamente, en la siguiente ruta de acceso:

-C:\tetra\Palieractif\Exe\SIP\.

#### 1.3.2 C:\tetra\Palieractif\Exe\SIP\Bcucpl\

Buscar y copiar, en el CD de instalación, los archivos siguientes:

- FCPL\_EXE.exe

- FRM\_EXE.exe
- OST\_EXE.exe
- Install\_Bcucpl.bat
- OREF\_SYNC.exe
- Sync.ini

Pegar en la ramificación creado previamente, en la siguiente ruta de acceso:

-C:\tetra\Palieractif\Exe\SIP\Bcucpl\.

### 1.3.3 C:\tetra\Palieractif\Exe\SIP\FFSIP\

Buscar y copiar, en el CD de instalación, los archivos siguientes:

- LCPLSIP\_EXE.exe
- LUPLSIP\_EXE.exe
- OPAL.DLL
- PTLIB.DLL
- Install\_FFSIP.bat

Pegar en la ramificación creado previamente, en la siguiente ruta de acceso:

-C:\tetra\Palieractif\Exe\SIP\FFSIP\

### 1.3.4 C:\tetra\Palieractif\Exe\SIP\Agents\

Buscar y copiar, en el CD de instalación, los archivos siguientes:

- LFRTSIP\_SNMP.dll
- lfrtsip\_snmp.reg

### 1.3.5 C:\tetra\Palieractif\Exe\Outils\Pmon\

Buscar y copiar, en el CD de instalación, los archivos siguientes:

- PMON\_SER.exe,
- Install\_PMON.bat,
- PMON.ini.

Pegar en la ramificación creado previamente, en la siguiente ruta de acceso:

-C:\tetra\Palieractif\Exe\Outils\Pmon\.

1.3.6 C:\tetra\Palieractif\DI\

-Copie todos los archivos DLL en el directorio DLL (CD de instalación) en el directorio C:\tetra\Palieractif\DI\.

#### 1.4 Instalación de los servicios

##### 1.4.1 Instalación de la BCUCPL, FFSIP y servicios PMON

En C:\tetra\Palieractif\Exe\SIP\Bcucpl\ access path, double click Install\_Bcucpl.bat file.

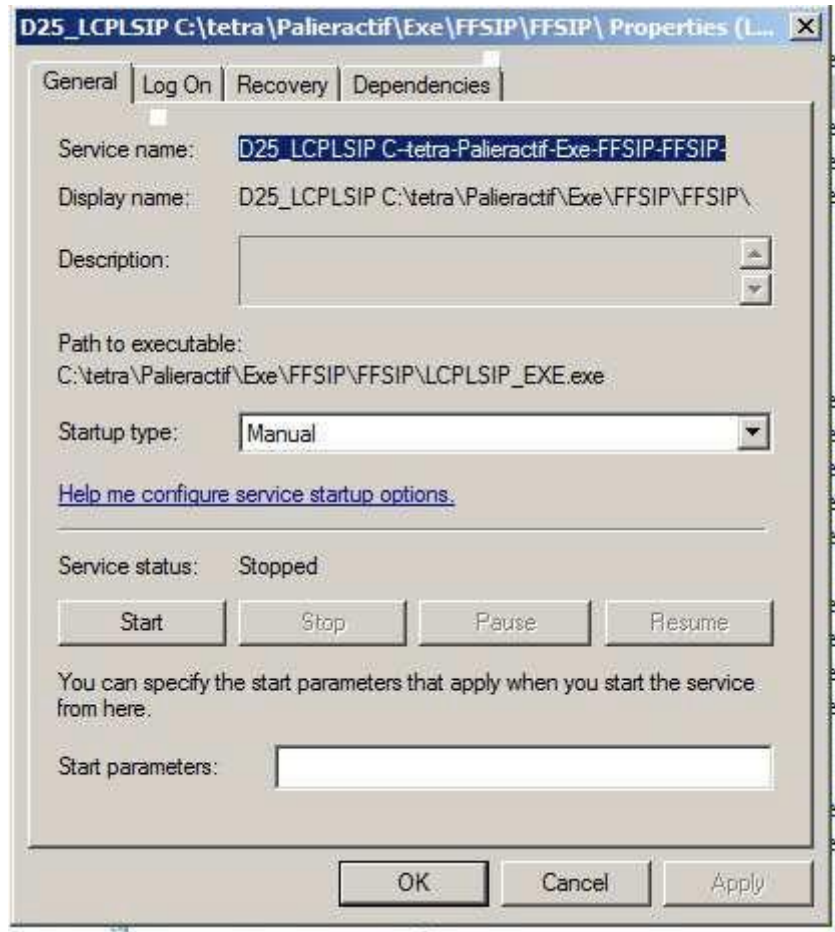
En C:\tetra\Palieractif\Exe\SIP\FFSIP\ access path, double click Install\_FFSIP.bat file.

En C:\tetra\Palieractif\Outils\Pmon\ access path, double click Install\_PMON.bat file.

Haga clic en el icono Mi PC con el botón derecho del ratón, apunte menú Administrar.

Doble clic en Servicios y aplicaciones, haga clic en Servicios (la lista de los servicios que aparece en la sub-ventana de la derecha).

Haga un clic derecho en cada servicio instalado y señalar la opción Properties (por ejemplo, "D25\_LCPLSIP").



**FIGURA 3.5** “Servicio D25\_LCPLSIP. General”

Haga clic en la lista desplegable Tipo de inicio y elegir la opción Manual, a continuación, haga clic en Aceptar.

Nota: Haga la misma operación para todos los servicios, excepto para el servicio de la tarde en la que se tiene que quedar en la ingeniería de control automático.

#### 1.4.2 Instalación de los servicios AGENCIAS

- Haga doble clic en el archivo ' lfrsip\_snmp.reg ' en el directorio C: \ tetra \ Palieractif \ Exe \ FFSIP \ Agents \ ruta.

- Haga clic en icono Mi PC con el botón derecho del ratón y seleccione el menú Administrar.

#### 1.5 Actualización de archivo Pmon.ini

En el directorio C: \ tetra \ Palieractif \ Outils \ PMON \ ruta de acceso, haga doble clic en el archivo PMON.ini. En la columna [SERVICIOS], modifique el número de servicios que se han visto: " NB = 7". Escriba las líneas siguientes:

```
-SERVICE 1 = D25_FCPL C--Tetra-Palieractif-Exe-SIP-  
Bcucpl-
```

```
-SERVICE 2 = D25_FRM C--Tetra-Palieractif-Exe-SIP-  
Bcucpl-
```

```
-SERVICE 3 = D25_OST C--Tetra-Palieractif-Exe-SIP-  
Bcucpl-
```

```
-SERVICE 4 = D25_OREF_SYNC C--Tetra-Palieractif-Exe-  
SIP-Bcucpl-
```

```
-SERVICE 5 = D25_LCPLSIP C--Tetra-Palieractif-Exe-SIP-  
FFSIP-
```

```
-SERVICE 6 = D25_LUPLSIP C--Tetra-Palieractif-Exe-SIP-  
FFSIP-
```

```
-SERVICE 7 = SNMP
```

•Back-up y cierre el archivo PMON.ini.

#### 1.6. Actualización de archivo Frontal.ini

```
#####  
# FRONTAL FILAIRE SIP DIGICOM 25 : commentaires et remplissage #  
#####  
[RESOURCE]  
TYPE=LINE  
NUMBER_LINE_RESOURCES=10  
[PABX] DISA = 59  
RTCP_PATH = 0  
RECORD = 0
```

```
MASTER = 1
MASTER_ADDR=203.1.1.90
RESOURCES=2
[SIP] LISTENER_PORT=5061 REGISTRAR_TIMER=15
REGISTRAR_ADDRESS=203.1.1.90
LISTENER_ADDRESS=203.1.1.90
REGISTRAR_USER_NAME=3000
REGISTRAR_AUTH_NAME=3000
REGISTRAR_AUTH_PASSWORD= GAIN_PCM_OUT=7.0
GAIN_PCM_IN =0.5
[PING_CONF] TEMPO_FOR_PING=10 NUMBER_OF_PING=3
[SELNAME] SITE=SIPGTW1
#[RESOURCE]
# Type de frontal à renseigner
#TYPE = SUPERVISOR
# Stand alone
#NUMBER_LINE_RESOURCES = 16
[HOSTS]
# Adresse du process SCPL interface FCPL
BSCC=203.1.1.90
# Non utilisé pour un dispatcher
BSCU=203.1.1.89
# Adresse du BCU interface intersite C Plane
FRTC=203.1.1.90
# Adresse du BCU interface intersite U Plane
FRTU=203.1.1.90
# Adresse du BCU interface intersite OMC
OMCS=203.1.1.90
# Adresse du process FRM
FRM=203.1.1.90
# Adresse du serveur OREF
OMCR=203.1.1.50
# Non utilisé
```

```
GROUP_SERVER=127.0.0.1
INTER=127.0.0.1
# Adresse du process AIOM interface SCPL
AUDIO=203.1.1.90
[SERVICES]
# Port d'écoute SCPL pour la connexion de DIGICOM25 DISPServer
#SCPL_IHM=6000
# Port d'écoute FRM pour la connexion de SCPL
#SCPL_FRM=5001
# Port d'écoute AIOM pour la connexion de SCPL
#SCPL_AUDIO=5002
# Port d'écoute AIOM pour la connexion de AIO
#PORT_AUDIO_SERVER = 7000
# Identique
CPLANE_BUPL=2500
CPLANE_OMC=3200
UPLANE_OMC=3201
FRM_OMC=3202
INTER_CC=3250
CPLANE_FRM=3300
UPLANE_FRM=3301
# Port UDP sockets IPMC traffic INTER_UPL=3302
# Port UDP sockets IPMC alternat, debut/fin de comm, libération
INTER_FRM=3303
INTER_SDS=3304
INTER_FCPL=3305
OMCS_OMCR=3500
UPLANE_BSC=10501
CPLANE_BSC=10727
OMCS_OMCS=3002
[PARAMETERS]
# Mode stand alone
SITE_NUMBER = 16
```



```

BS_NUMBER = 6
GATEWAY = 16777191
MAIN_ADDRESS=203.1.1.90 [OMC]
RESTORE_BD = 0
TEST_BD_REF = 0
TEST_BD_ST = 0
DUMP_BD_ST = 1
# Path for BD and DTS directories
BD_PATH = C:\tetra\palieractif\exe\SIP\BD
DTS_PATH = C:\tetra\palieractif\exe\SIP\DTS
[OPERATION] SUPERVISION_SNMP = 1
STAND_ALONE = 0
RESTORE_BD = 0
[SYNC]
# Connection Port between OST and OREF_SYNC
OMCS_SYNC_PORT=3501
[TICKET]
# Connection Port between OST and OREF_TICK OMCS_OMCTICK = 3522
# Defines how often the OST send its tickets to the NMS (OREF_TICK process).
#value is in seconds.
TICKETS_PERIODICITY = 5
# Defines how many tickets are sent to the NMS (OREF_TICK process).
MAX_TICKETS_TO_SEND = 50

```

### 3.2.2 Configuración del Servidor Asterisk

Lo primero que debemos hacer es obtener una versión de Asterisk Now, se puede descargar de <http://www.asterisknow.org/>, que es software desarrollado por Digium, se trata de una distribución de Linux especialmente adaptada para hacer funcionar Asterisk en cuestión de minutos ya que viene con todos los requerimientos y dependencias de software pre configurados y permite la administración y mantenimiento del servidor de una manera realmente sencilla.

Cuando lo descargáis de la Web es una imagen ISO, que solo nos hace falta un grabador para quemar dicha imagen.

Si arrancamos el PC, con el CD introducido no saldrá una primera pantalla

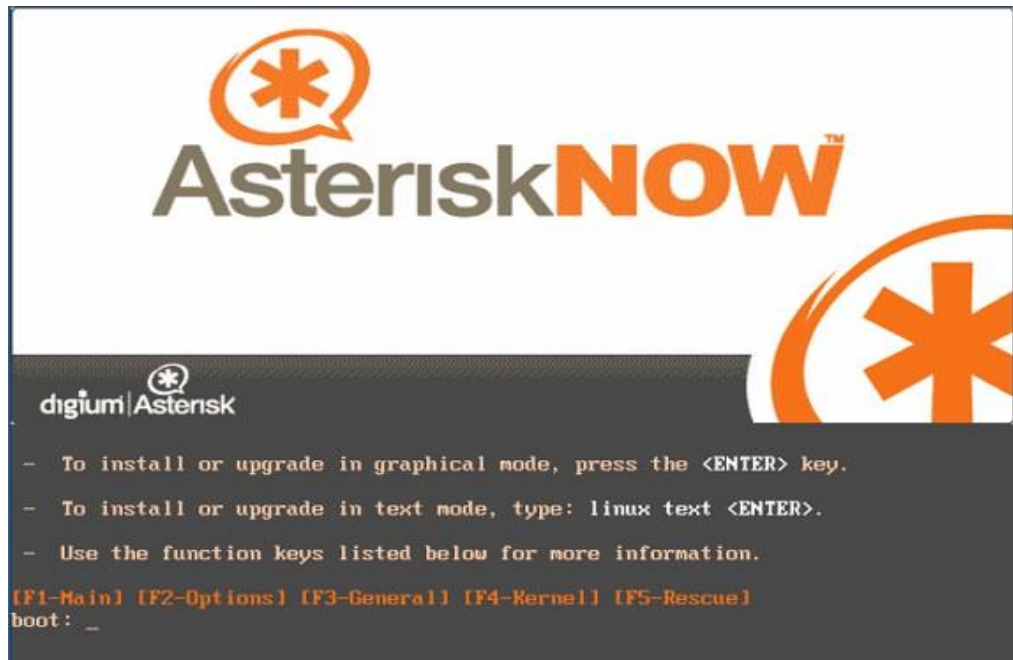


FIGURA 3.6 “pantalla instalación asterisk”

Donde pulsaremos enter para hacer la instalación en modo gráfico. Nos saldrá una pantalla dándonos la bienvenida a la instalación.

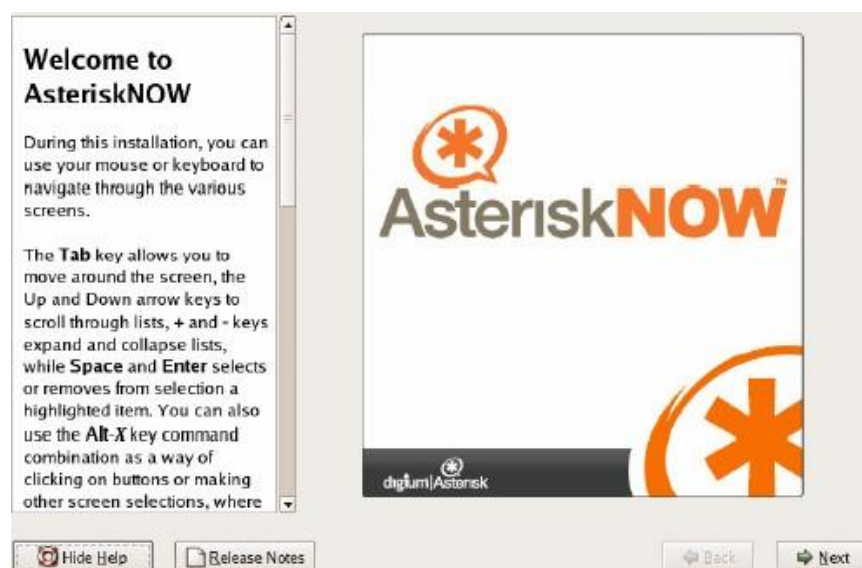
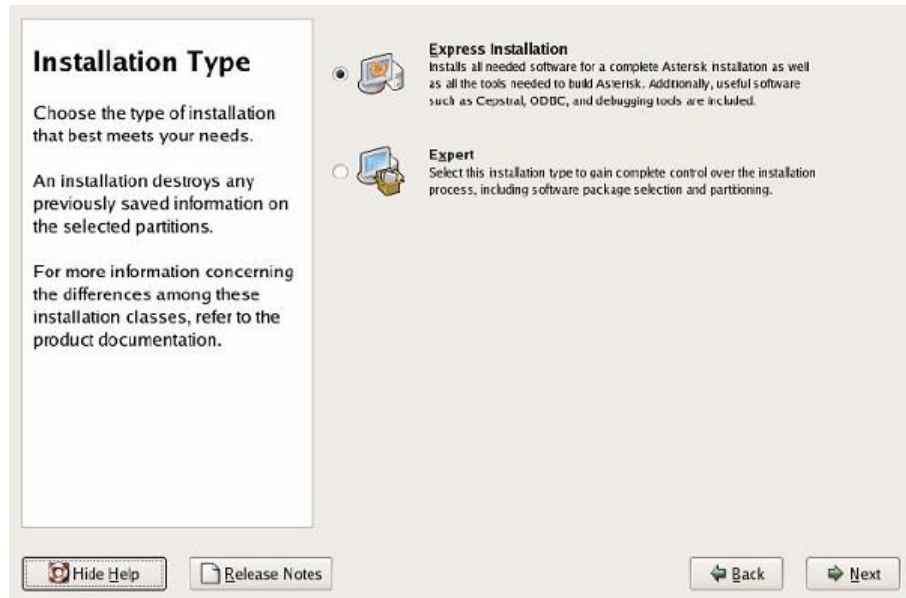


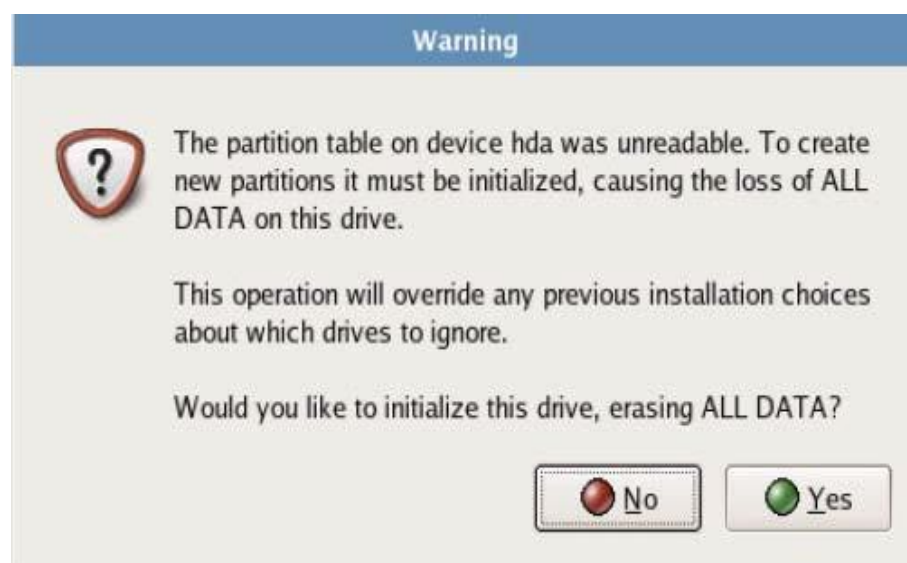
FIGURA 3.7 “pantalla instalación asterisk”

Donde deberemos pulsar el botón Next. Nos saldrá la siguiente pantalla, donde seleccionaremos la opción de Express installation y pulsamos Next.



**FIGURA 3.8** “pantalla instalación asterisk”

La siguiente pantalla puede variar. Si en el disco donde deseamos realizar la instalación de Asterisk Now, existe la instalación de un Windows, nos saldrá un mensaje indicando que se borrarán todos los datos. Donde deberemos pulsar yes.



**FIGURA 3.9** “pantalla instalación asterisk”

Ahora empezara el proceso de partición automático. Donde dependiendo de nuestro caso deberemos seleccionar la primera o segunda opción, y pulsar next.

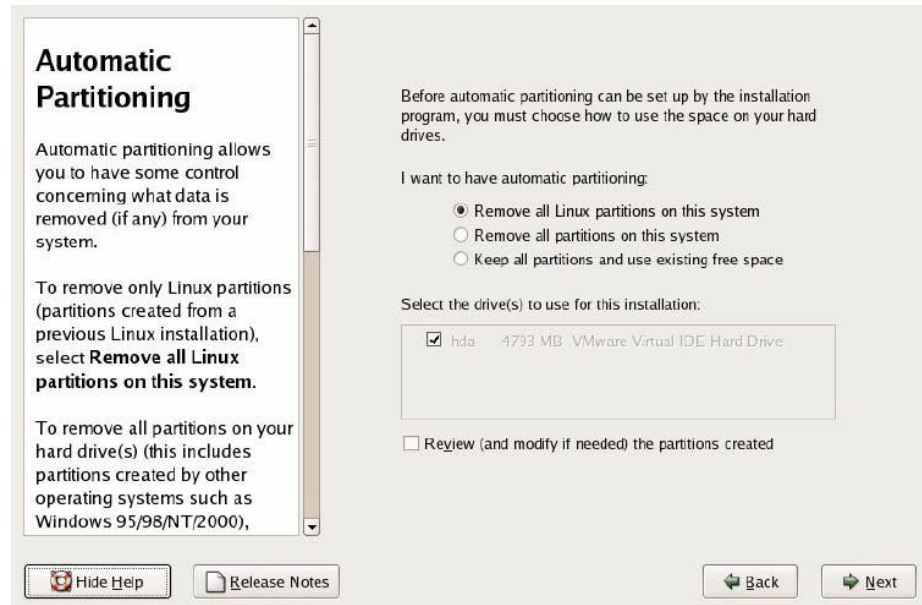


FIGURA 3.10 “pantalla instalación asterisk”

Antes de empezar el proceso de instalación, saldrá un mensaje indicando que si estás seguro de eliminar las particiones. Donde pulsamos yes.

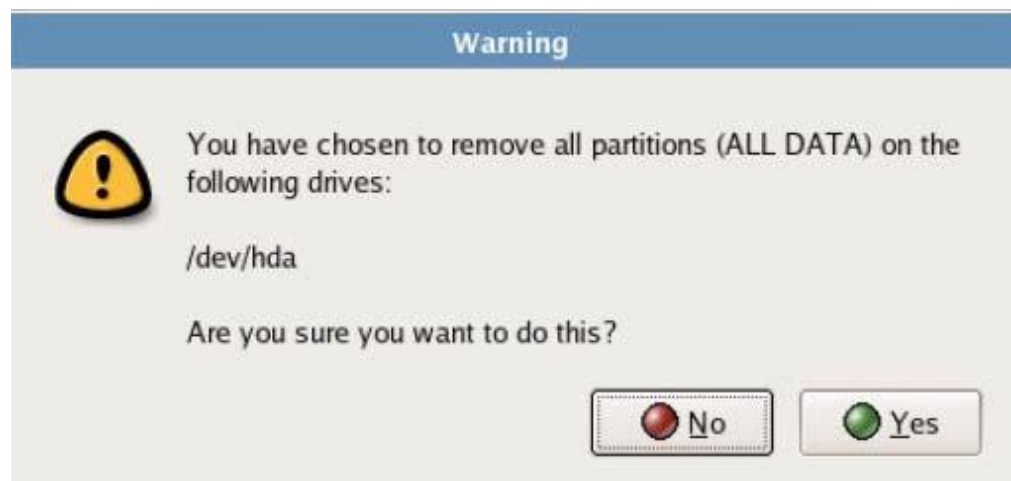


FIGURA 3.11 “pantalla instalación asterisk”

La siguiente pantalla es para configurar la red en nuestro servidor Asterisk. Donde se puede configurar mediante DHCP (obtención automática de datos) o manualmente.

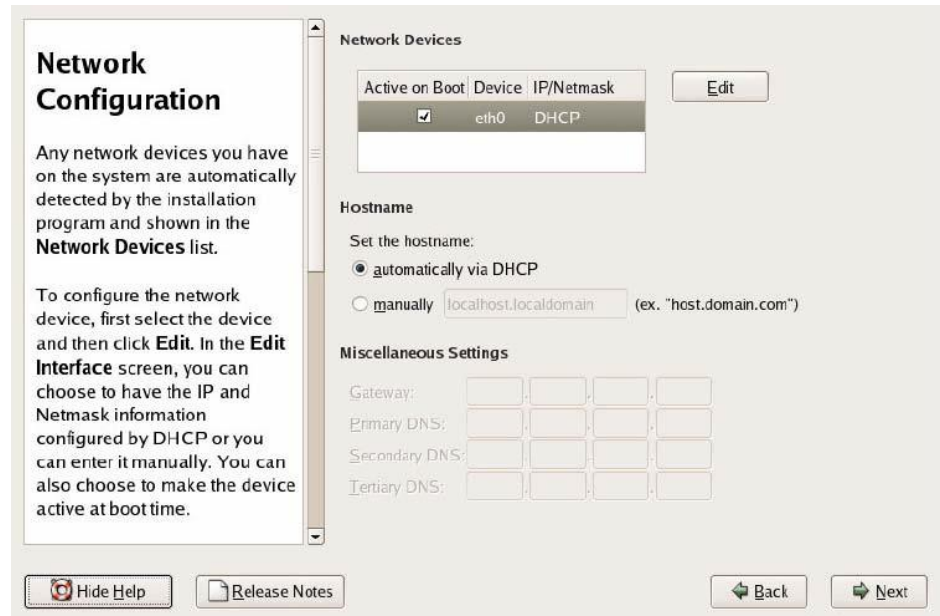


FIGURA 3.12 “pantalla instalación asterisk”

La siguiente pantalla es para configurar la zona de tiempo. Que dependiendo de las zonas donde vivamos, deberemos seleccionar una u otro.

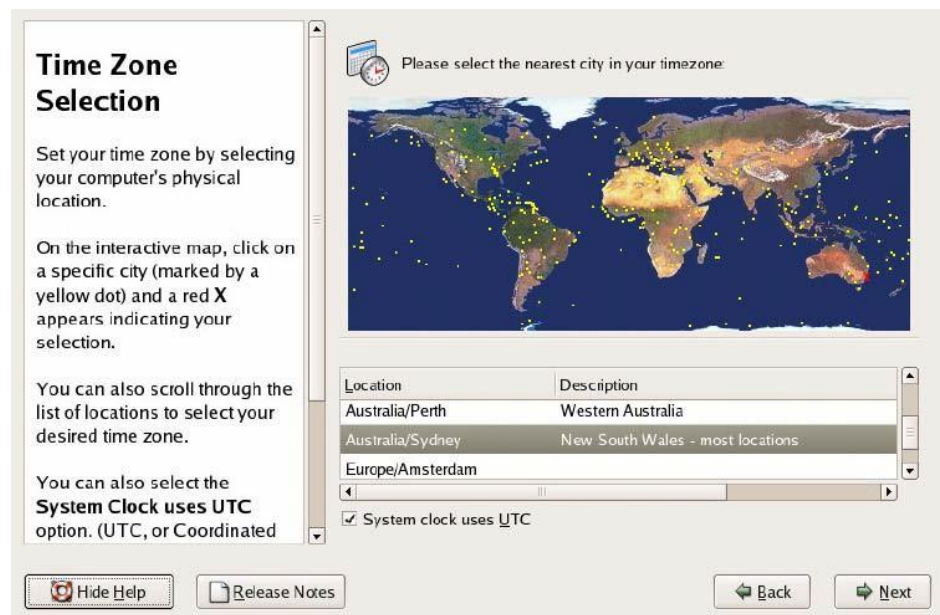


FIGURA 3.13 “pantalla instalación asterisk”

Por defecto se crea un usuario que se llama ADMIN, donde en la siguiente pantalla nos solicita la contraseña. Este será el administrador de la parte del asterisk, pero también existe el usuario ROOT que es el administrador de todo. Y pulsamos next.



FIGURA 3.14 “pantalla instalación asterisk”

Antes de comenzar la instalación, nos muestra una pantalla que nos indica procesos que se llevan a cabo en la instalación. Pulsamos next.



FIGURA 3.15 “pantalla instalación asterisk”



Antes de realizar la instalación, se debe realizar el formateo del sistema.



**FIGURA 3.16** “pantalla instalación asterisk”

Luego comienza el proceso de instalación, que nos saldrán las siguientes pantallas.



**FIGURA 3.17** “pantalla instalación asterisk”



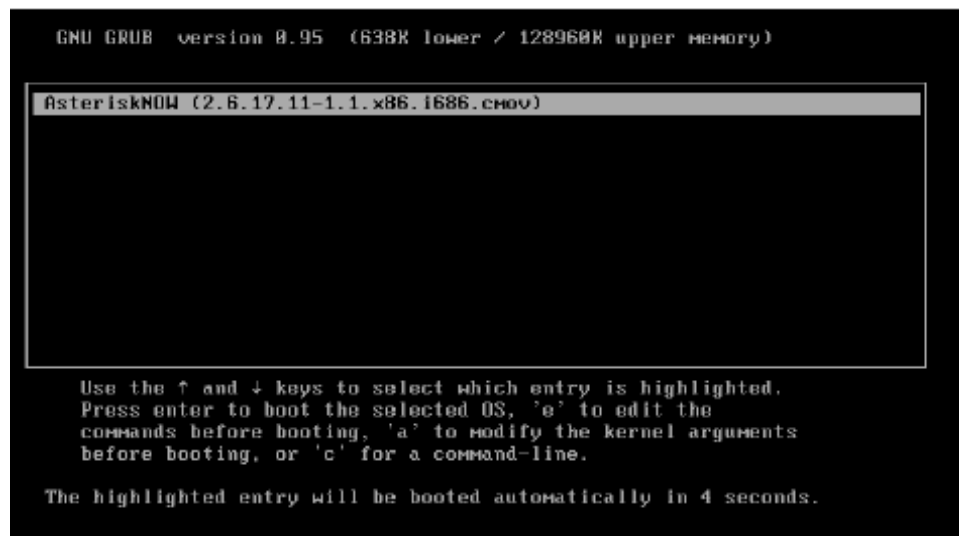
**FIGURA 3.18** “pantalla instalación asterisk”

Una vez finalizada la instalación, nos solicitara el reinicio

### **Primer arranque del Asterisk Now**

Una vez finalizada la instalación, se ha reiniciado el PC, donde nos mostrara una pantalla que nos solicitara el núcleo de arranque. En un principio solo habrá uno.





**FIGURA 3.19** “arranque asterisk”

La pantalla siguiente nos saldrá en el primer arranque de Asterisk Now, donde nos indica que existe un usuario llamado admin., y que su contraseña la hemos introducido durante el proceso de instalación.



**FIGURA 3.19** “arranque asterisk”

Por último, el PC se quedara con la consola de Asterisk Now. Donde si deseamos podemos actualizar el sistema. El proceso de actualización será de varios minutos.



**FIGURA 3.19** “actualización asterisk”

### Administración del Asterisk a través de un navegador

Para ello, debemos tener un ordenador, con un navegador Web, donde introducimos la IP del servidor Asterisk. Donde cada vez, se nos solicitara si deseamos obtener un certificado para conectarnos. Esto provoca que todo lo que se transmita entre los dos PC sea de forma encriptada.



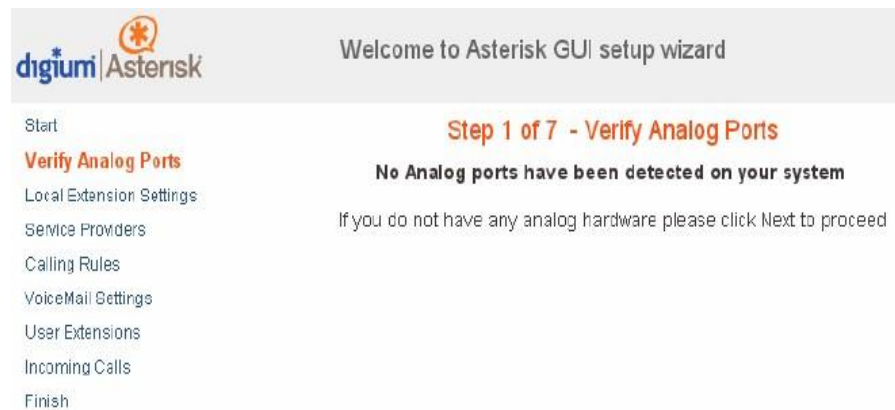
**FIGURA 3.20** “administración Web”

Lo siguiente que nos solicita es que introduzcamos el usuario ADMIN con su correspondiente contraseña.



**FIGURA 3.21** “administración Web”

La primera vez que entremos en el sistema Asterisk, se nos abrirá un asistente, que consisten en siete puntos. Donde se configuran los parámetros del funcionamiento, pero este tutorial realizara la configuración a partir de los ficheros de texto.



**FIGURA 3.22** “administración Web”

### Asignación de la contraseña al usuario Root

Para realizar la configuración a través de la edición de los ficheros de configuración, en algunas ocasiones, necesitaremos ser el usuario Root. Para ello, en la pantalla inicial, en la parte superior izquierda. Esta la opción de System Configuration.



**FIGURA 3.23** “configuración Root”

Donde nos solicitará que debemos introducir el usuario admin con su correspondiente contraseña.

A sign-in form with a white background and a blue header bar containing the text "Sign In". Below the header, there are two input fields: "User Name:" followed by a text box, and "Password:" followed by a text box. At the bottom of the form is a blue button with the text "Sign In" and a right-pointing arrow.

**FIGURA 3.24** “configuración Root”

Habrà un menú en la parte izquierda de la nueva pantalla que nos presenta, donde en el menú Configuration, y dentro de el, en el submenú Root password. Podremos asignar una contraseña a nuestro usuario Root.

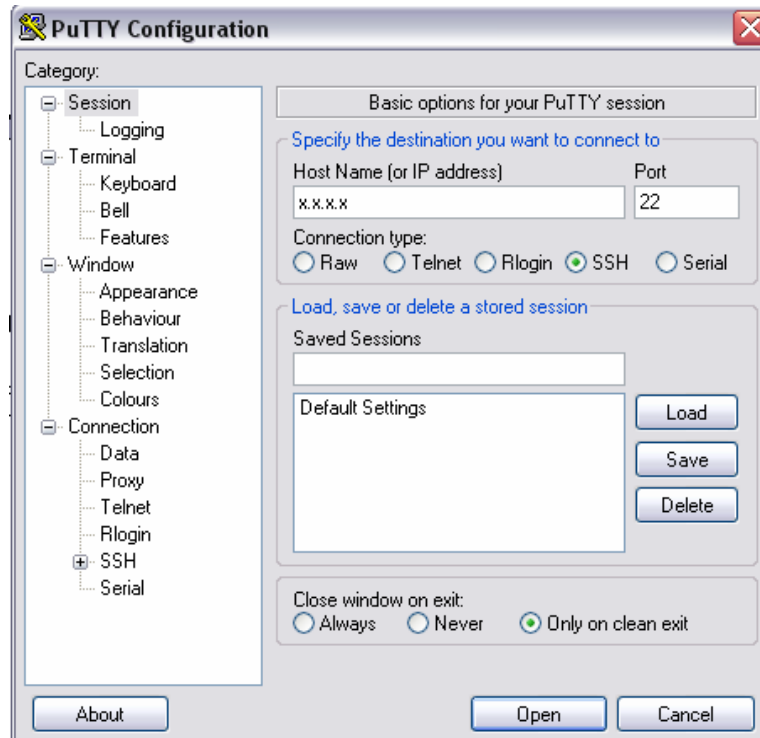
A screenshot of a web interface. On the left is a vertical navigation menu with a blue header bar. The menu items are: Appliance Logs, Backup and Restore, Change Password, Configuration, Configure Conary, Configure Email, Configure Networking, Configure Notification, Configure Proxy, and Root Password (which is highlighted). To the right of the menu is the "Change root User Password" page. It has a title "Change root User Password" and a sub-header "To change the system's root user password, enter and confirm the new password." Below this is the instruction "Click OK to complete the password change." There are two input fields: "New Password" and "Confirm Password". At the bottom left of the form is a blue button labeled "Learn More", and at the bottom right is a blue button labeled "OK".

**FIGURA 3.25** “configuración Root”

Además se puede configurar otros elementos sobre nuestro sistema.

### **Conexión a nuestro servidor**

Para ello debemos conectarnos a nuestro servidor para poder trabajar, se puede utilizar un programa llamado Putty. Donde el tipo de conexión debe ser SSH y donde pone Host Name o Ip Adress, debemos introducir la IP del servidor.



**FIGURA 3.26** “configuración servidor”

Se nos abrirá una consola, donde nos solicitará un usuario para hacer login. Donde introduciremos el usuario admin con su correspondiente contraseña. Si deseáramos para a usuario Root, debemos introducir el comando “su” e introducir la contraseña de Root.

```
login as: admin
admin@192.168.8.104's password:
Last login: Tue May 8 13:13:29 2007 from 192.168.
[admin@centralita ~]$ su
Password:
[root@centralita admin]#
```

**FIGURA 3.27** “configuración servidor”

Los ficheros de configuración de Asterisk se encuentran en la ruta /etc/asterisk

### Configuración de SIP.CONF

En este fichero se definirán los usuarios, con sus correspondientes extensiones, numero a marcar para realizar una llamada.

Para realizar un comentario se deberá anteponer en la línea un  
“.”  
; .

## USUARIO EJEMPLO

Para definir la extensión, de deberá poner entre corchetes.

[numero de extension]

Definimos el tipo de extensión. Esta "user" se usa para autenticar llamadas entrantes, "peer" para llamadas salientes y "friend" para ambas

type=friend

Definimos la contraseña que tiene la extensión

secret=contraseña

Para definir que el tiempo de latencia no sea mayor que 2 seg.

qualify=yes

Si el dispositivo utiliza Nat

nat=no

El modo que se transmite los tonos

dtmfmode=info

Permitir al usuario conectarse de diferentes PC

host=dynamic

No permite conexión directa entre dos usuarios, siempre pasara  
por

Asterisk

canreinvite=no

Nombre del contexto definido en extensions.conf

context=nombre

Correo de voicemail definido

mailbox=correo

Define un grupo de llamadas

callgroup=1

Define el grupo de llamadas válidas para una aplicación pickup

pickupgroup=1

### **Configuración de EXTENSIONS.CONF**

En este fichero se define el contexto de las extensiones que hemos definido en sip.conf. Además, de indicar las acciones que se van a producir cuando le llame a una extensión.

Ahora vamos a ver un par de ejemplos prácticos para entender el funcionamiento.

En este ejemplo se van a definir tres contextos.

- [pstn-in]; llamadas entrantes de línea telefónica
- [outgoing\_calls]; llamadas salientes de línea telefónica
- [innova]; llamadas internas de la empresa

Primero vamos a definir el contexto de llamadas entrantes. La definición para que pstn-in sea el contexto de llamadas entrantes será definida más adelante.

Nombre del contexto de las llamadas entrantes

[pstn-in]

Pone a disposición las extensiones internas

include => dominio

Segundo vamos a definir el contexto de llamadas salientes. Donde la definición del contexto lo veremos más adelante.

Nombre del contexto de las llamadas salientes

[outgoing\_calls]

Permite llamadas nacionales a fijos de Telefónica

```
exten => _9XXXXXXXX,1,Dial(Zap/1/${EXTEN})
```

Permite llamadas a móviles nacionales

```
exten => _6XXXXXXXX,1,Dial(Zap/1/${EXTEN})
```

Para colgar la llamada

```
exten => t,1,Hangup()
```

Tercero vamos a definir el contexto de llamadas internas. Aquí es importante que pongáis el mismo nombre que el parámetro context del fichero sip.conf. En el siguiente ejemplo que para capturar las llamadas externas

Nombre del contexto

[dominio]

Aquí se enumeran por orden de sucesión. Donde lo primero es preguntar

```
exten => s,1,Answer
```

Lo segundo que la espera sea de cero segundos

```
exten => s,2,Wait,0
```

Lo tercero que llame a la extensión 7000 durante 15 segundos. Donde Ttr, es para darle permiso de transferir llamadas y para que suene una música mientras se espera en la llamada

```
exten => s,3,Dial(SIP/7000,15,Ttr)
```

Si la anterior extensión no ha cogido el teléfono, se llamara durante

Si las dos extensiones anteriores no cogen el teléfono, saltara en buzón de voz de la extensión 7000



exten => s,5,VoiceMail(7000@innova)

Se colgara la llamada

exten => s,6,Hangup

### 3.2.3 Configuración en el NMS para la llamada TETRA – ASTERISK

El propósito de este tercer paso es describir la configuración de un SIP Gateway en la red TETRA utilizada.

#### 3.2.3.1 Configuración OIHM

Line gateway form		BTS	Parameters	Timer	Line Gateway	DDI
Frontal type	<input type="radio"/> PABX		<input checked="" type="radio"/> H323			
DISA number	<input type="text"/>		Number of codec resources supported	<input type="text" value="8"/>		
PSTN path	<input type="text"/>					
Gatekeeper						
IP	<input type="text" value="203.1.1.87"/>		Timer	<input type="text" value="15"/>		
Port	<input type="text" value="1720"/>					
Login	<input type="text"/>		<input type="button" value="Password"/>			

#### 3.2.3.1.1 Formulario de Equipo Gateway

**Figura 3.28** Línea formulario Equipo de Gateway

El SIP Gateway está configurado en el OIHM como un frontal Línea.

Parámetros:

- Frontal Type: seleccione VOIP para configurar el equipo de puerta de enlace de línea como un gateway SIP.
- DISA number: no se utiliza en esta versión.
- PSTN path: no se utiliza en esta versión.

- Number of codecs resources: es el número máximo de llamadas simultáneas que se podría conseguir en el puerto seleccionado en el frontal.
- La sección Gatekeeper sólo se utiliza para la puerta de enlace H323.
  - IP: no se utiliza para SIP GW pero se tienen que llenar los campos, incluso si no se utilizan estos campos.
  - Puerto: no se utiliza para SIP GW pero se tienen que llenar los campos, incluso si no se utilizan estos campos.
  - Login: no se utiliza para SIP GW pero se tienen que llenar los campos, incluso si no se utilizan estos campos.
  - Timer: no se utiliza para SIP GW pero se tienen que llenar los campos, incluso si no se utilizan estos campos.

### 3.2.3.1.2 Formulario SDA (PSTN DDI)

The screenshot shows a web-based configuration interface titled "Line gateway form". It has a navigation bar with tabs: "Line gateway form" (active), "BTS", "Parameters", "Timer", "Line Gateway", and "DDI".

The main content area contains a table with the following data:

Start	End	Label
3000	3100	test

Below the table, there are input fields for configuration:

- Label: test
- Start: 3000
- End: 3100
- Prefix: 016052
- ISSI: 201 3000
- Description: (empty text area)

On the right side of the interface, there are several action buttons: "Add" (with a plus icon), "Delete" (with a minus icon), and "Save" (with a floppy disk icon).

Parámetro

**Figura 3.29** Formulario SDA

Se tiene la lista de los números reservados para sus teléfonos IP, los números a marcar de terminan en 3001-3100 y desea asociarlas a los números de TETRA, entonces usted tiene que usar este formulario.

Campo de inicio: Esta es la primera extensión, en nuestro caso 3000.

Campo Final: Esta es la última extensión, en nuestro caso 3100.

Base y ISSI: si el teléfono IP es el 3002, el número a marcar en el TETRA será 201 3002.

### 3.2.3.1.3 Puerta de enlace suscriptor

También es necesario crear una nueva PABX Gateway suscriptor que sea utilizada por el SIP Gateway.

ISSI	Label
16777191	PABX Gateway
16777193	H323 Gateway
16777199	SIP Gateway

**PABX gateway subscriber form**

ISSI: 16777199  Infrastructure invalidation

Label: SIP Gateway

Organization: Super-Organization [Organization properties](#)

Registration site: SIP GATEWAY [Organization TSI ranges](#)

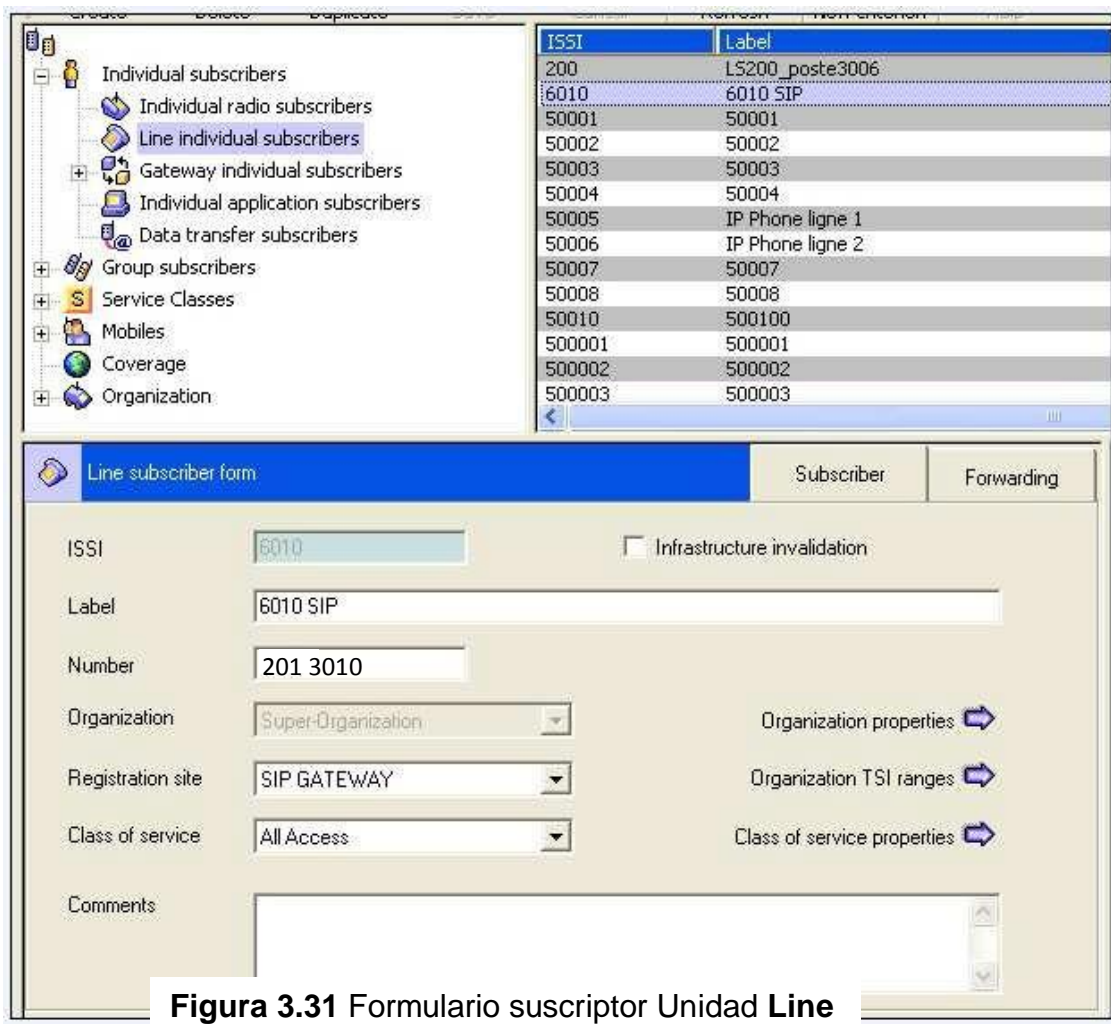
Class of service: All Access [Class of service properties](#)

Forwarded gateway:

Number:

### 3.2.3.1.4 U| **Figura 3.30.** Formulario de suscriptor Gateway

Si desea asociar un teléfono IP con una dirección de Tetra, hay que crear una nueva Unidad de Línea de Suscripción. Se escribe el número de teléfono IP.



### 3.2.3.2 Los Tipos de Llamada

### 3.2.3.2.1 Llamada IP saliente

El Gateway SIP utilizado es el 1 677 7199

Desde un terminal TETRA, para llamar a un teléfono IP.

Marque el número de teléfono IP.

Número marcado: 201 3010 (No hay modo de prefijo)

El numero marcado será buscado en el OIHM (NMS) donde será encontrado con un el Isis 6010, este es un número (ID) que está registrado en el SIP Gateway el cual marcara el enlace suscriptor <16777199>, y la extensión a llamar <201 3010>.

La puerta de enlace SIP marcará:

Número enviado al servidor Asterisk IP: <201 3010>

### 3.2.3.2.2 Llamada IP entrantes

Se marcar un prefijo en el teléfono IP antes de que el número ISSI, este prefijo no debe ser transmitido con el número ISSI a la puerta de enlace. Si un prefijo se utiliza (por ejemplo, 7), usted tendría que:

Número marcado: <760332>

Número de llamada: <201 3010>

El número marcado: <60332>

La puerta de enlace recibirá el número que llama <201 3010> y el número llamado <60332>.

Como el número del Teléfono IP está configurado como una abonado en e NMS, el número que aparecerá en el terminal tetra será el 6010.

### 3.2.3.3 Archivo de configuración Frontal.ini

[SIP]

# Listener address of SIP GW

```
LISTENER_ADDRESS=203.1.1.88
# Address of the IPBX
REGISTRAR_ADDRESS=203.1.1.87
# Login name to connect to the SIP GW
REGISTRAR_AUTH_NAME= 3000
# Not used (no password implemented)
REGISTRAR_AUTH_PASSWORD=
# Listening port for the gw
(5061) LISTENER_PORT=5061
# Try to connect every 15 seconds
REGISTRAR_TIMER=15
# Increase or decrease volume TETRA -> SIP
GAIN_PCM_OUT=7.0
# Increase or decrease volume SIP -> TETRA
GAIN_PCM_IN=0.5
# client SIP user name
REGISTRAR_USER_NAME =3000
```

### 3.3 REVISION Y CONSOLIDACION DE RESULTADOS

La revisión que se dio en una demostración en laboratorio, el representante de la mina comprobó que si se podía dar la solución que ellos requerían tal cual, así superarían algunas falencias ya presentadas en la comunicación por falta de equipos asignado, o simplemente porque su radio se descargó y estaba en su oficina concentrado en papeles, así ya lo podrían llamar a su teléfono de oficina.

## CONCLUSIONES

Esta propuesta para lograr hacer interactuar el estándar TETRA con la tecnología de comunicación Volp a través del Asterisk, nos permite concluir:

1. El estándar TETRA, no solo nos garantiza una comunicación de calidad con su propia tecnología, si no que demuestra tener una escalabilidad con otras tecnologías que también se han vuelto estándares como lo es el protocolo SIP.
2. El protocolo SIP se ha vuelto ya desde hace más de una década en un protocolo de confianza, aprovechado que muchas tecnologías lo toman como un estándar, agregándola a sus posibles funcionalidades , al también tener una confiabilidad de seguridad al utilizar el puerto 5061, que pide identificación al iniciar la sesión de comunicación.
3. Tanto el Estándar TETRA como el protocolo SIP poseen un sistema de identificación durante la comunicación, al igual que no se saturan transmitiendo todo el dato de un comienzo, si no que utiliza la señalización para primero buscar su camino de la data, para luego ser transmitida.
4. La implementación se daría de forma rápida, ya que se tendría las facilidades en acceso a la plataforma del estándar TETRA de comunicación de la mina, al igual que su Data Center el cual cuenta con un tendido de Fibra, para su comunicación IP.

## RECOMENDACIONES

Para mejorar esta propuesta de interacción entre el estándar TETRA la Telefonía Voip - Asterisk, se recomienda lo siguiente:

1. El estándar TETRA junto con el Asterisk, usando el protocolo SIP, se complementan bien, según su requerimiento de la minera, bajo esta premisa, se le recomienda el uso de ambos en combinación, ya que se podía utilizar otros protocolos diferentes al SIP pero que no prestarían la misma calidad de servicio ni la seguridad deseada de la comunicación.
2. El protocolo SIP siendo el más recomendado para ser el puente entre el estándar TETRA y el Asterisk tiene que ser usado, explotando su seguridad, usando el puerto 5061, que es el que tiene seguridad, mas no el 5060 que no la tiene.
3. se recomienda usar en toda su tecnología instalada y por instalar protocolos que usen la señalización de la data, ya que como en este caso, la combinación del TETRA y el Asterisk (usando SIP) tienen a favor la señalización en la comunicación lo que la hace más rápida y confiable.
4. en el Data Center ubicado en el NOC principal se encontrara el Servidor asterisk, así como el Servidor SIP-GW, al tener la facilidad en las instalaciones, se recomienda instalar una redundancia del servidor



Asterisk así como del servidor Sip-Gw, ya que estos actuarían como un respaldo adecuado para las comunicaciones en caso de alguna emergencia fortuita.