Universidad Zaragoza
1542

# Trabajo Fin de Grado

## ESTUDIO DE LAS CENTRALES DE VOIP EN DOTACIÓN EN EL EJÉRCITO DE TIERRA QUE OFREZCAN MEJOR SERVICIO Y SEGURIDAD A LAS NECESIDADES DEL ET TENIENDO EN CUENTA LOS CONDICIONANTES OPERATIVOS Y TÉCNICOS ACTUALES


Autor

Iván Ayala Serrano

Directores:

Dr. Carlos E. Cajal Hernando

Cap. Ricardo Simón Serna

Centro Universitario de la Defensa-Academia General Militar


Año 2016

## Agradecimientos

Primero de todo quiero agradecer a mi familia el apoyo recibido durante los cinco años en los cuales he conseguido superar el Grado de Ingeniería de Organización Industrial así como el especial apoyo recibido durante los últimos dos años a la que ya considero parte de mí. Sin vuestro apoyo bien sabéis que esto no habría sido posible

Seguidamente quiero agradecer a todo el Batallón II/I toda la ayuda que he recibido durante la realización de mis prácticas destinas a la creación de mi Trabajo Fin de Grado. Desde el Teniente Coronel por darme la oportunidad de ir a su batallón pasando por la compañía de puesto de mando de cuyo jefe, el Capitán Ricardo Simón Serna, mi tutor militar, he recibido no sólo enseñanzas destinadas al Trabajo Fin de Grado sino también para mi futuro militar. Agradecer también a toda la sección de Red Básica de Área las enseñanzas recibidas durante mi estancia, tanto al Teniente al mando Don Alfonso Bógalo Chaparro como a sus suboficiales los Sargentos primero Alonso Merino, Sergio, por la ayuda recibida en cuanto a la configuración de las centrales y los problemas que pudieran aparecer, y Moliner Tapia, Ignacio por sus conocimientos en cuanto a gestión de las centrales y creación de los puestos de mando y los sargentos Pacheco Jiménez, Adrián, por la ayuda recibida al comienzo de las prácticas en cuanto a los conocimientos generales de Voz sobre IP y Castillo López, Antonio, por haber estado ayudándome en toda la realización del proyecto y la creación de las maquetas para el ancho de banda, muchas gracias, sin vuestra ayuda este Trabajo Fin de Grado no habría podido realizarse. No quiero olvidar tampoco al resto de cuadros de mando de la compañía, tanto de la sección OTAN con los temas relacionados a los medios para transmitir la información, como a los de la sección SIMACET que acogieron mis preguntas acerca del cifrado de la comunicación. Debo recordar también a la compañía de apoyo del citado batallón en la cual fui gratamente recibido por sus cuadros de mando y me solucionaron todas aquellas dudas que me pudieran surgir en cuanto a los medios satélite o la central Call Manager en cuanto a su gestión y puesta en marcha.

Por último quería agradecer a mi tutor el Dr. Carlos E. Cajal Hernando toda la ayuda recibida durante la realización del presente trabajo, así como las innumerables horas que me ha dedicado en sus correcciones. En este apartado no quería olvidar a aquellos profesores a los que he pedido ayuda en la realización del mismo, muchas gracias. También quiero agradecer a todos aquellos profesores su apoyo cuando por las circunstancias a lo largo de mi estancia en la Academia General Militar tuve que pedirles ayuda sin olvidar a aquellos que sin pedírsela me la ofrecieron desinteresadamente.

Muchas gracias a todos y cada uno de vosotros este trabajo es la muestra del sacrificio, dedicación y aprendizaje de estos últimos e intensos cinco años.

## Resumen

El fin último de este trabajo fin de grado es el de analizar las centrales de trabajo de Voz sobre IP (VoIP) en dotación en el Ejército con el objetivo de discernir cuál de las centrales se ajusta en mayor medida a las necesidades actuales del Ejército de Tierra teniendo en cuenta las características y especificaciones que un equipo de comunicaciones debe tener para su uso en las Fuerzas Armadas. Para ello se estudia de manera general los fundamentos básicos de la VoIP para posteriormente hacer un estudio de las centrales en dotación en el Ejército. En el análisis que se realiza sobre las centrales se estudian los aspectos clave de la VoIP en el Ejército como ancho de banda, seguridad, gestión, servicios y presupuesto necesario para la puesta en marcha. Finalmente se concluye el trabajo fin de grado con un juicio crítico sobre las pruebas y ejercicios realizados. En la última parte del trabajo se exponen las conclusiones sacadas durante la realización del mismo en cuanto a la importancia crítica de la Voz sobre IP para el futuro del Ejército, la urgente necesidad de modernización de los sistemas de comunicación de la Red Básica de Área y las conclusiones extraídas en cada una de las pruebas de campo realizadas, así como la propuesta de líneas futuras de trabajo para hacer de la VoIP una realidad en el Ejército.

## Abstract

The main aim of this final degree project is to analyze the systems of Voice over IP (VoIP) supplied in the Army in order to discern which of them is more suitable to the current needs of the Army keeping in mind the features and specifications that a communication equipment must have to be used in the Armed Forces**.** To get that objective, the basis of VoIP has been studied briefly to make later a study of the systems supplied in the Army. In the analysis performed about the systems it has been studied key aspects of VoIP in the Army, as bandwidth, security, management, services and budget needed for the implementation**.** Finally, the final degree project is concluded with a critical judgment about the tests carried out. In the final part of this project it has been included the conclusions achieved during its realization regarding the importance of Voice over IP for the future of the Army**,** the urgent need for modernize the communication systems of Basic Area Network and the drawn conclusions in each field trial, as well as the writing of some future lines of study to make VoIP a reality in the Army.

# Índice de contenidos

## Acrónimos

| | |
|---|---|
| FAS | Fuerzas Armadas |
| RBA | Red Básica de Àrea |
| BT | Batallón de Transmisiones |
| PC | Puesto de mando |
| PM | Policía Militar |
| CT | Centro de Transmisiones |
| VHF | Very High Frequency (Muy Alta Frecuencia) |
| VoIP | Voz sobre IP |
| IP | Internet Protocol (Protocolo de internet) |
| Códec | Codificador-Decodificador |
| QoS | Quality of service; Calidad del servicio |
| UIT | Unión Internacional de Telecomunicaciones |
| SIP | Protocolo de Inicio de Sesión |
| HTTP | Protocolo de transferencia de Hipertexto |
| MCU | Multipoint Control Unit (Unidad de Control Multipunto) |
| IETF | Internet Engineering Task Force ( Grupo de trabajo de Ingeniería de Internet) |
| SIMACET | Sistema de Información para el Mando y Control del Ejército de Tierra |
| CBR | Constant Bit Rate (tasa de bit constante) |
| VBR | Variable Bit Rate (tasa de bit variable) |
| CECOM | Centro de Comunicaciones |
| CGFUL | Cuartel General de la Fuerza Ligera |
| TN | Territorio Nacional |
| CGES | Centro de Gestión de Sistemas |
| RCT | Red Conjunta de Telecomunicaciones |

C.A.C Iván Ayala Serrano

# 1 Introducción

Las Fuerzas Armadas (FAS) se encuentran inmersas en un periodo de actualización continuo con el fin de dar a la sociedad un servicio óptimo en cuanto a cooperación, seguridad y defensa se refiere. Dentro de este proceso, ocupan un puesto relevante las transmisiones. Esta especialidad fundamental es considerada pieza clave en cuantas misiones puedan desarrollar las FAS. Esto es debido a que el cometido principal de las transmisiones es conseguir enlazar los puestos de mando con el elemento a pie facilitando su labor.

Cabe resaltar la importancia que tiene en todo este proceso la información. Como en toda gran empresa es preciso y necesario que la información fluya tanto de los escalones superiores al subordinado en forma de órdenes como en sentido inverso a través de informes para que el mando pueda ejercer su labor. El Ejército al tener una serie de características especiales debe tener un sistema de información seguro y confiable. En ningún caso puede asumirse el riesgo de que no haya enlace en un momento determinado entre los puestos de mando y sus subordinados. Por ello la necesidad de innovación constante con el objetivo de la mejora del servicio es una realidad en nuestras unidades de transmisiones.

Una de las áreas de investigación sería la encauzada para la renovación del sistema de comunicaciones actual en la Red Básica de Área (RBA). Esta renovación pasaría por la implantación de un nuevo sistema de comunicaciones basado en Voz sobre IP para de esta manera reemplazar el antiguo debido a su estado de obsolescencia. Este trabajo tiene como fin analizar las características que una central de Voz sobre IP (VoIP) debe tener para servir en el Ejército de Tierra, así como la comparación de las dos centrales actuales de VoIP con el objetivo de discernir cual de dichas centrales se ajusta en mayor medida a nuestras necesidades.

## 1.1 Objetivos y alcance del proyecto

El objetivo para este Trabajo Fin de Grado ha sido marcado después del estudio de los diferentes medios de VoIP con los que cuenta el Ejército de Tierra en la actualidad. En cuanto a los medios disponibles de VoIP, el Batallón de Transmisiones II dispone de dos centrales totalmente diferentes, por un lado la central proporcionada por la empresa Cisco llamada Call Manager y por otro la central desarrollada por la empresa Digium llamada Asterisk. Si bien es cierto, ambas centrales se encuentran en esta unidad a modo de prueba dando servicio en las maniobras, pero a nivel Ejército se debe encontrar una solución a esta dualidad debido al gasto ineficiente de presupuesto y la

dificultad que plantea el tener dos estaciones diferentes para el uso de la VoIP desde el punto de vista de la instrucción. Por ello el objetivo marcado para este Trabajo Fin de Grado ha sido la elección de una de estas dos centrales, para de manera única hacer uso de la VoIP a través de la misma y en un futuro sustituir a la actual RBA en estado de obsolescencia. El alcance del Trabajo Fin de Grado sería el estudio de ambas centrales en los puntos críticos para su explotación dentro del ámbito del Ejército de Tierra con el fin de la elección de una de ellas en base a las pruebas realizadas. Además se redactarán las características que debe cumplir una central de VoIP para su servicio en el Ejército de Tierra.

## 1.2 Metodología

Para llevar a cabo este Trabajo Fin de Grado se ha utilizado la siguiente metodología en las prácticas externas desarrolladas en el Batallón de Transmisiones II/I de Madrid. Primeramente se ha llevado a cabo una recopilación de información mediante entrevistas a personal de la unidad y profesores de la Academia General Militar. Posteriormente el trabajo se centró en un análisis de la información recopilada para sintetizarla y estudiarla para asentar los conocimientos básicos y comprender los problemas ocurridos debidos a la dualidad. Seguidamente se realizó un aprendizaje de cada una de las centrales de VoIP en la unidad para comprender el funcionamiento de las mismas así como sus ventajas y vulnerabilidades frente a la otra central. También ha existido una fase de pruebas de campo la cual ha ocupado la mayor parte de las prácticas al centrarse el estudio en torno al resultado de dichas pruebas. Para ello se realizaron maquetas con la debida configuración de cada una de las centrales con sus respectivos medios, se estudiaron los despliegues de los puestos de mando así como se analizó el planeamiento y juicio crítico de las maniobras sobre las cuales se realizaron dichas pruebas con el fin de analizar la seguridad en torno a cada una de las centrales y finalmente se estudió la puesta en marcha de cada una de las centrales en cuanto al presupuesto necesario para su utilización. Para terminar el trabajo se analizó el resultado de dichas pruebas con el fin de extraer las conclusiones y líneas futuras de estudio oportunas.

## 1.3 Estructura de la memoria

La memoria ha sido redactada de tal manera que cualquier persona pueda entender el trabajo sin necesidad de conocimientos previos sobre el temario. Por ello la primera parte de esta memoria es la introducción, en la cual se explica la importancia que tienen las transmisiones para el Ejército. Se debe tener en cuenta que al hacer uso de la tecnología se encuentra en un periodo de actualización continuo. También se expone de manera breve el problema en el cual se encuentran las transmisiones debido a ese periodo de actualización ya que al probar nuevas tecnologías hacen acopio de diferentes equipos provocando dualidad en los medios en dotación siendo necesario este Trabajo Fin de Grado para discernir entre los mismos cuales son los idóneos para el trabajo. Seguidamente y de manera general se explican los conceptos básicos para entender la VoIP, conocimientos necesarios para comprender la última parte del Trabajo Fin de Grado. En la tercera y última parte del Trabajo Fin de Grado se expone la comparación entre las dos centrales de VoIP en dotación en el Ejército de Tierra. En esta parte se comparan los puntos principales en el ámbito militar de las dos centrales en cuanto al servicio que estas deben prestar al Ejército para de esta manera comprobar cuál de ellas es capaz de dar un rendimiento superior con el mínimo desembolso económico.

# 2 Comunicación oral sobre protocolo IP (VoIP)

Se debe considerar este apartado como la base sobre la cual se sustenta todo el trabajo, ya que previo al estudio de las diferentes centrales en dotación en el Ejército de Tierra se deben tener unos conocimientos mínimos de VoIP. En este capítulo se estudiarán las generalidades seguidas del funcionamiento así como de los terminales necesarios y una serie de normas y requisitos que tiene la VoIP para su correcta explotación.

## 2.1 Generalidades de VoIP

Para entender qué es la VoIP se debe pensar primero en su antecesora, la telefonía tradicional. La telefonía tradicional nació con un claro propósito: permitir la comunicación entre dos usuarios transmitiendo la información entre ellos [1]. Este sistema de comunicaciones era analógico, primera gran diferencia con el nuevo sistema digital de comunicación. El usuario no encontrará ninguna diferencia en la comunicación ya que seguirá realizando los mismos pasos para comunicarse con otro usuario que con el sistema antiguo. Pero para el sistema, y como se explicará en profundidad en los sucesivos apartados, el proceso es totalmente distinto. La principal ventaja de este nuevo modelo de comunicación será el enrutamiento automático. Inicialmente existía una única línea de comunicación entre dos puntos, si esa línea se veía afectada el enlace entre esos dos puntos caía. Sin embargo, con el nuevo modelo todo ha cambiado. Existen una serie de nodos a lo largo de la red que le dan forma y seguridad a la comunicación. En líneas generales estos nodos forman distintos caminos entre dos puntos. Inicialmente, gracias a diferentes protocolos, se utiliza el camino más corto o de menos coste entre los dos puntos, pero si este enlace se ve afectado automáticamente y sin que el usuario se vea afectado, la red encontraría otro camino que permitiese la comunicación entre esos dos puntos. De esta manera la VoIP se ha transformado en el futuro de las comunicaciones. Para la empresa que proporciona el servicio, previo desembolso inicial, prácticamente lo obtenido son beneficios ya que integra varios servicios (internet y llamadas telefónicas) en uno sólo debido a la unificación de la estructura [2].

## 2.2 Funcionamiento

El funcionamiento de la VoIP se dividirá en diferentes partes. Primeramente se explicará la manera de digitalizar la voz. Seguidamente se hará referencia al transporte de los datos por la red.

Posteriormente se expondrán los componentes necesarios para la formación de una red de VoIP y por último se aclararán los protocolos y estándares finalizando con los conceptos básicos de calidad de servicio.

### 2.2.1 Códec

Como se ha mencionado anteriormente una de las grandes diferencias entre la VoIP y la telefonía tradicional, es que la VoIP lleva a cabo un proceso digital. Por ello es necesario un proceso de digitalización de la voz para su posterior envió por la red, este proceso se realiza mediante una serie de técnicas genéricas como se puede apreciar en la tabla1. La VoIP utiliza una serie de estándares de codificación en función del ancho de banda del cual se disponga y la calidad de audio que se quiera enviar ya que estos dos últimos conceptos se encuentran directamente relacionados. A mayor calidad de audio, mayor ancho de banda a ocupar. Los estándares actuales más comunes en el mercado se pueden apreciar en la tabla 2.

Para codificar la voz existen una serie de técnicas genéricas [3]:

| ***TÉCNICA*** | ***CARACTERÍSTICAS*** |
|---|---|
| DE FORMA DE ONDA | Muestrean la señal analógica y la codifican directamente. Tienen buena calidad pero a costa de necesitar más ancho de banda que otras técnicas para reconstruir la señal en el terminal destinatario. |
| VOCODER O BASADA EN LA FUENTE | Representa la onda sonora conforme a un modelo matemático convenido entre origen y destino. No se transmite la información de la voz, sino los parámetros que la definen. Su principal ventaja es el pequeño ancho de banda necesario. |
| HIBRIDOS | Aprovechan las virtudes de los dos anteriores ofreciendo buena calidad sonora con anchos de banda limitados. |

Tabla 1. Técnicas genéricas de codificación.

Para agrupar los diferentes métodos de codificación de la voz existen una serie de estándares, entre los cuales para VoIP destacan [2]:

| ESTANDAR | CAUDAL COMPRIMIDO | CALIDAD | CARACTERÍSTICAS |
|---|---|---|---|
| G.711 | 64 Kbit/s | Calidad - Voz a 64 Kbps | Fue el primer estándar desarrollado para la codificación de la señal de voz, ancho de banda de 3 kHz a 64 kbps. Es el esquema de codificación básico para la mayoría de los sistemas de comunicación multimedia. |
| G.722 | 48 - 64 Kbit/s | Calidad - Voz a 48 Kbit/s | Este estándar fue desarrollado para lograr una codificación de una señal de audio de mayor calidad con ancho de banda de 7 kHz a 48, 56, y 64 kbps. |
| G.723 | 5.3 ó 6.3 Kbit/s | Calidad - Voz a 6.3 Kbit/s | Fue desarrollado para aplicaciones de videoconferencia a caudales de bits menores de 64 kbps. El G.723. 1 es el estándar de facto para la codificación de voz en Internet. |
| G.728 | 16 Kbit/s | Calidad - Voz | Fue diseñado para caudales bajos. Con una calidad comparable al estándar G.721 pero usando un caudal comprimido 4 veces inferior. |
| G.729 | 8 Kbit/s | Calidad - Voz | La motivación para su creación fue su uso en redes inalámbricas. |
| GSM | 13 Kbit/s | Calidad - Voz | Con una calidad inferior a la familia G.72X. Es específico de la telefonía móvil. |
| iLBC | 8 Kbit/s | Superior a G.729 | Se trata de un códec de gran calidad de voz con un consumo reducido de ancho de banda, su principal desventaja es el alto consumo de recursos de la CPU. |
| Speex | 8, 16, y 32 Kbit/s | | |
| DoD CELP | 4 y 8 Kbit/s | | |
| SILK | 6 a 40 Kbit/s | | |
| DVI | 32 Kbit/s | | |

Tabla 2. Estándares de codificación de voz.

### 2.2.2 Transporte

En cuanto al transporte de los mensajes de voz de un usuario a otro se debe tener en cuenta si estos usuarios hacen uso de una única red, la red IP, o por el contrario están haciendo uso de dos redes diferentes, red IP y, por ejemplo, red telefónica tradicional (analógica). En el primero de estos casos el transporte se realizará de una manera más sencilla explicada en el anexo correspondiente. En el segundo de los casos será más complejo debido a que se necesitará el uso de determinados terminales los cuales llevan asociados una serie de protocolos para la “traducción” entre las diferentes redes usadas. Tanto estos terminales como los protocolos, van a ser explicados en profundidad posteriormente en sus respectivos apartados.

## 2.3 Principales componentes de VoIP

Un sistema de VoIP genérico está formado por tres componentes [4]:

- *Cliente*: Es el componente que inicia, establece y termina las llamadas de voz. Es el encargado de codificar, empaquetar y transmitir los mensajes de voz enviados por el usuario "llamante" al igual que se encarga de recibir, decodificar y reproducir los mensajes de voz del usuario "llamado".
- *Servidor*: Es el componente con la función de gestión de la red. Entre algunas de sus misiones se encuentran: validación de usuarios, enrutamiento, registro de usuarios, distribución de utilidades, etc.
- *Pasarela*: También llamado Gateway, este componente actúa de "traductor" entre las diferentes redes. Lleva a cabo la interconexión de aquellas redes con protocolos y arquitecturas diferentes.

## 2.4 Protocolos y estándares

En el momento que surgió la VoIP surgió la necesidad de la existencia de una serie de reglas o normas que dictaran como debía fluir la comunicación entre los diferentes terminales de VoIP para que entre ellos pudieran entenderse. De esta manera los usuarios podrán transmitir la información entre ellos sin percatarse del proceso que se está llevando a cabo. En este apartado se darán ejemplos de los protocolos más famosos y utilizados por los diferentes sistemas. Se debe tener en cuenta que existen multitud de ellos, tanto genéricos como específicos creados por las empresas para sus propios sistemas de VoIP. Dentro de los genéricos, los protocolos más conocidos son [3]:

1. H.323: Es el más genérico siendo compatible con la telefonía tradicional pudiéndose usar entre terminales conectados a distintas redes.
2. SIP: Creado con posterioridad al H.323 siendo más específico centrándose sólo en la comunicación entre dos terminales en la misma red de internet.

## 2.5 Calidad del servicio

Para entender este punto se debe volver a centrar la atención en la telefonía tradicional y su futuro. Para que la VoIP sea la sustitución de la telefonía tradicional se debe dar el servicio como mínimo con la misma calidad que el sistema anterior [5]. La calidad del servicio (QoS) está directamente relacionada con el retraso y el ancho de banda, los dos factores fundamentales con los cuales se mide su calidad son [2]:

- Calidad de voz extremo a extremo: factor determinado por la codificación – decodificación de la voz y la pérdida de paquetes de información que conforman los mensajes.
- Retardo extremo a extremo: Como ya se ha explicado hay multitud de procesos desde que el cliente comunica al micrófono su mensaje hasta que el mismo llega al otro usuario, tales como digitalización de la voz, codificación, procesos para poder ser enviados esos paquetes por la red, etc. Todo este proceso puede requerir un tiempo determinado que afecta a la comunicación con un retardo que no puede ser mayor a 150 ms al ser éste el umbral de lo permitido.

# 3 Medios en dotación en el Ejército de tierra de VoIP

En esta última parte del trabajo se realizará la comparación entre las dos centrales de VoIP que tiene en dotación el Ejército de Tierra. En la actualidad el Batallón de Transmisiones II de Madrid (BT II) se encuentra en la puesta en marcha de esta nueva tecnología para la sustitución de la antigua RBA. Para ello la unidad ha sido dotada con dos centrales diferentes para trabajar con VoIP. Por un lado la central Asterisk de Digium y por otro la central Call Manager de Cisco.

Lo primero que se debe aclarar es el concepto genérico de central. Una central es la manera con la cual se nombra a los diferentes elementos centrales indispensables para la creación de una red de VoIP. En el caso de la central Asterisk sería necesario un ordenador con la instalación previa del servidor y en el caso de la central Call Manager directamente sería el router el que contendría el servidor al tener en su interior el software necesario para su funcionamiento.

## 3.1 Importancia de la VoIP en el Ejército

En los últimos años el Ejército está llevando a cabo una modernización dentro de sus sistemas comunicación. En concreto uno de los puntos más importantes sería la modernización de los equipos con los cuales forma la Red Básica de Área (RBA), red a través de la cual forma el nivel más básico de enlace necesario para la acción del mando. Esta RBA se empezó a implantar a partir de 1996 y debe ser sustituida por la VoIP debido a las siguientes razones:

1. Unificación de los servicios: La principal misión de las transmisiones es facilitar la labor del mando con un enlace rápido, eficaz y de sencilla utilización. Hasta ahora el mando se veía obligado a adaptar su trabajo a los servicios que les proporcionaba las transmisiones. De manera inicial las transmisiones montaban la RBA, uno de los teléfonos de esta red era extendido hasta la mesa del General. Seguidamente se levantaban los enlaces satélite y las transmisiones debían extender de nuevo otro teléfono hasta la mesa del General y por último si se contaba con el apoyo de un Centro de Comunicaciones (CECOM) las transmisiones volvían a poner un tercer teléfono en la mesa del General para su enlace con la Red Conjunta de Telecomunicaciones (RCT), red que comunica todos los Acuartelamientos, Bases y Establecimientos militares en Territorio Nacional. Con la antigua RBA podían unificarse los servicios a través de pasarelas y de esa manera usar un único teléfono, pero si fallaba la RBA dejaba de

funcionar todo. Como puede observarse, en un intento de dotar al mando de enlace, lo que se conseguía era la saturación del mismo debido a la gran cantidad de medios diferentes para extender su acción. Sin embargo, este problema desaparecería gracias a la VoIP. El modo de funcionamiento de esta nueva red sería extender un único teléfono al mando y posteriormente conectar el router al que está conectado dicho teléfono a los router que llevan las estaciones Rioja para usar la RBA. Al router de las estaciones Antequera para el uso del enlace satélite y, por último, la conexión de este router a través de tarjetas FXO a un CECOM para su conexión con la RCT. El mando simplemente necesitaría un listín telefónico con el cual saber las extensiones de cada puesto de mando para comunicarse sin llegar a saber qué tipo de red estaría utilizando en cada momento, de esta manera gracias a la VoIP se unificarían las diferentes redes montadas en un único teléfono facilitando la acción del mando, objetivo último de las transmisiones.

2. Eficacia en el encaminamiento de la información: Esto es debido al uso del enrutamiento automático propio de las redes de internet. Con el antiguo sistema de enlace el mando se veía afectado en todo momento por la caída de alguno de los sistemas de RBA o satélite ya que debía ser avisado del no funcionamiento de uno de estos sistemas y debía usar los otros mientras durara la reparación. Sin embargo, con la VoIP el mando será ajeno de todos estos problemas debido a que el enlace estará por duplicado e incluso por triplicado de manera que al mismo router al que están conectados todos los teléfonos del puesto de mando están conectadas las tres redes de RBA, satélite y CECOM, por tanto y gracias al enrutamiento automático si uno de estas redes cae la información de manera automática será encauzada por otra de las redes mientras se soluciona el problema ocurrido en la primera.

### 3.2 Problemas debido a la dualidad

Una vez aclarado el término genérico de central y habiendo comprobado la importancia que tiene la VoIP para el futuro de las comunicaciones dentro del Ejército de Tierra, se debe analizar el problema de la dualidad en los medios en dotación en el Ejército. La dualidad en el Ejército es sinónimo de un uso ineficiente de los medios y del presupuesto que se le otorgan debido a los siguientes motivos:

1. *Instrucción mal planificada o ineficiente*: Debido a la utilización de dos centrales diferentes para el trabajo con VoIP, la instrucción que reciben los cuadros de mando y la tropa es en

muchos casos incompleta ya que deben saber configurar dos centrales para, dependiendo las maniobras que se estén desarrollando, usar o la central de Asterisk o la central Call Manager. Por este motivo las horas necesarias para aprender a gestionar cada una de las centrales se duplica al tener que compatibilizar el estudio de una y otra central cada día. Los cuadros de mando y la tropa nunca llegan a tener un conocimiento total sobre ninguna de las dos centrales y además no pueden especializarse en ninguna de ellas al no saber de manera definitiva cuál de las dos centrales será finalmente la elegida.

2. *Presupuesto destinado a cursos de formación*: Este tipo de cursos tienen como fin la formación de los cuadros de mando y tropa en un área determinada. Dentro de la especialidad fundamental Transmisiones tienen gran relevancia debido a que para la puesta en marcha de las estaciones el conocimiento técnico es imprescindible. Siendo conscientes de la importancia de este tipo de cursos y teniendo en cuenta el reducido presupuesto destinado a tal efecto, estos cursos deben ser elegidos con sumo cuidado. Desde la parte que acontece a la VoIP estos cursos son realmente importantes debido al hecho de que la VoIP es el futuro de las transmisiones como relevo de la antigua RBA, pero al tener dos centrales diferentes sin saber cuál de las dos será finalmente la elegida, este dinero se está gastando de manera errónea al realizar cursos, por ejemplo, con la empresa Cisco para saber el funcionamiento de la central Call Manager sin tener certeza que esta central sea la definitiva.

3. *Mantenimiento*: Desde el punto de vista del mantenimiento y por ende de la logística, el hecho de que existan en dotación dos centrales para dar el mismo servicio de VoIP provoca que este servicio de mantenimiento funcione de una manera ineficaz por dos motivos:
    a. *Personal*: La instrucción recibida por parte de aquel personal encargado de solucionar los posibles problemas técnicos o las reparaciones que se deban hacer deberá instruirse en ambas centrales provocando de nuevo un uso ineficiente del tiempo y del presupuesto en conocer ambas.
    b. *Material*: De igual manera que en los puntos anteriores el gasto en material tendrá que ser por duplicado al tener dos centrales en vez de una para dar servicio con la VoIP, generando un uso del presupuesto de nuevo ineficaz.

Como se ha comprobado, la dualidad en el Ejército es un grave problema que se ha de erradicar, por ello se ha propuesto el análisis de las centrales en dotación en el Ejército para esclarecer cuál de ellas podrá dar un servicio más ajustado a las necesidades y capacidades del Ejército de Tierra.

## 3.3 Requerimientos técnicos de las centrales de VoIP

En este apartado se expondrán las diferentes pruebas realizadas así como el conocimiento técnico que se ha obtenido durante las prácticas externas con el fin de analizar las centrales de VoIP en dotación en el Ejército de Tierra.

### 3.3.1 Ancho de banda

El ancho de banda ha sido el primer punto a analizar ya que es un recurso crítico dentro de las maniobras o ejercicios realizados así como en las misiones del Ejército de tierra. Debido a las características de los medios de transmisión el ancho de banda es en muchos casos insuficiente, por ello este punto es tan importante en la comparación de las centrales. Con esta primera prueba se quiere comprobar qué central ocupará un menor ancho de banda por llamada realizada. Previo al estudio del ancho de banda necesitado por cada una de las centrales, se debe atender al medio por el cual se enviará esa información. Los principales medios para la comunicación entre diferentes puestos de mando con VoIP serían dos:

- Radioenlaces a través de estaciones Rioja-IP con antena modelo MT-3070: enlaces de 1 Mbps a una distancia aproximada de 40 Km.
- Enlaces satélite, con las estaciones ATQH y TLB-IP a velocidad 2 Mbps y estación Soria a velocidad 128Kbps, con distancia indefinida pudiendo enlazar con el satélite.

Además de contar con un escaso ancho de banda se debe tener en cuenta que no siempre se dispondrá de todo el ancho de banda para la transmisión de VoIP, sino que también se podrá compartir con otros sistemas propios del mando como el Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET).

Dentro del ancho de banda a ocupar en cada llamada, la mayor parte del mismo es ocupado por el códec del terminal usado. Dentro de cada central cabe la posibilidad de utilizar un códec u otro dentro de una pila de los códec que soporta.

Para las pruebas realizadas se ha utilizado el códec G.711ulaw. Este códec es el usado para los ejercicios y maniobras del BT II debido al buen resultado obtenido durante las mismas. El G.711ulaw utiliza un ancho de banda aproximado de 64 Kbps siendo independiente el terminal usado. Aun así

se debe tener en cuenta que cada central utiliza un protocolo diferente para comunicarse con los terminales, en el caso de Asterisk, el protocolo usado para comunicarse con el terminal es el protocolo SIP mientras que en el caso de Call Manager el protocolo usado para comunicarse con terminal cisco sería SCCP. Es importante tener en cuenta el protocolo usado debido a que cada protocolo tiene un sistema de señalización diferente en la realización de la llamada, por ello aunque el códec sea el mismo, el ancho de banda usado por cada central sería distinto.

Las pruebas han sido realizadas durante la preparación de las maquetas para las maniobras “Dragón” del año 2016. Para ello fue desplegada la sección de RBA dentro del cuartel bajo idénticas circunstancias que se encontrarán durante dichas maniobras.

Con ambas centrales fue dado de alta un ordenador como si se tratase de un terminal de VoIP más a usar durante las maniobras. Para la realización de las prácticas han sido utilizados los programas Zoiper y Cisco Communicator para emular un terminal de VoIP y de esta manera poder realizar o recibir llamadas a cualquier otro terminal de la red y el programa Wireshark para el estudio del ancho de banda ocupado por las llamadas.

Los resultados de las pruebas fueron los siguientes:

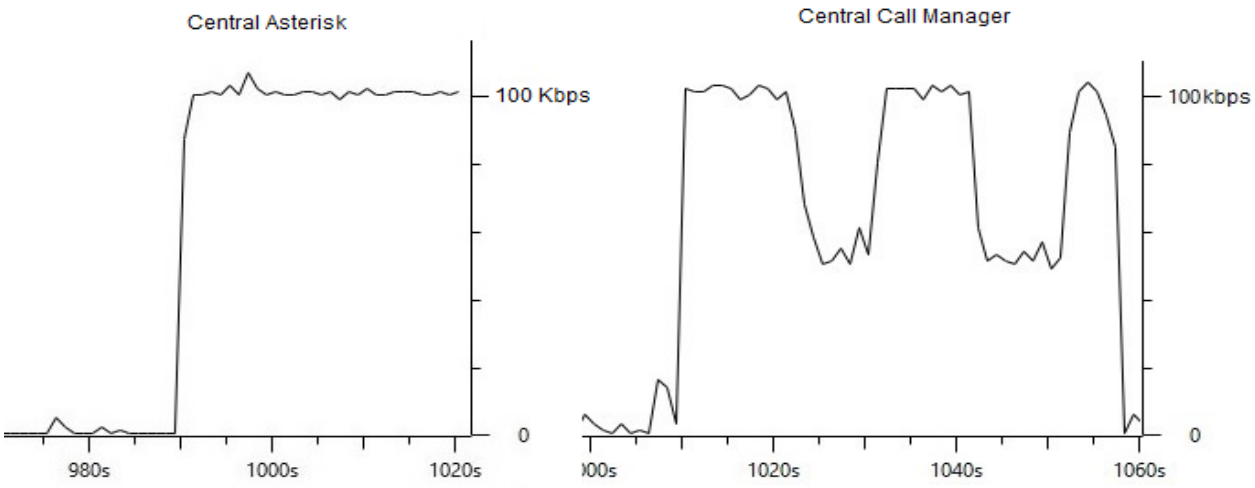



Figura 1: Comparación del ancho de banda de las centrales

Como puede observarse en la Fig. 1 el resultado obtenido difiere de lo esperado. En ambas centrales el protocolo de señalización ocupa durante la transmisión de información 100 kbps pero la principal diferencia entre ambas sería la cantidad de ancho de banda ocupado durante los silencios.

A la central Asterisk le correspondería un modo de codicación CBR (tasa de bit constante) el cual ocupa de manera continua desde el inicio hasta el fin de la llamada 100kbps. Sin embargo a la

central Call Manager le correspondería un modo de codificación VBR (tasa de bit variable) el cual ajusta el ancho de banda ocupado a la cantidad de datos a enviar, por ello durante los silencios el ancho de banda desciende hasta el 50%.

### 3.3.2 Seguridad

Dentro del Ejército en cuanto al trato de información la seguridad es uno de los factores más importantes. A priori siempre será más seguro una central de código cerrado como es la central Call Manager de Cisco frente a la central de código abierto como Asterisk. Esto es debido a que la propia empresa Cisco garantiza que su sistema tiene cierta garantía en cuanto a la vulnerabilidad. Pero para poder discernir entre una de las centrales en cuanto a la seguridad que aporta no sólo se debe atender a las garantías que da la empresa, sino que también se debe estudiar la manera en la cual se trata la información y la manera en la cual viaja por la red.

Para ello se dividirá el transporte de la información en dos apartados:

1. Desde el Centro de Transmisiones al Puesto de Mando: Para que se pueda entender el apartado de seguridad, se utilizará el despliegue de las maniobras Dragón (Fig. 2) como ejemplo, siendo dicho despliegue similar al resto de despliegues en cuanto a la formación de los puestos de mando (PC).


Figura 2: Despliegue maniobras Dragón.

Como puede observarse en la Fig. 2 el PC1 y el Centro de transmisiones 1 (CT1) que le da servicio no se encuentran a más de 100 metros. La seguridad a esta zona en concreto quedaría de la siguiente manera:

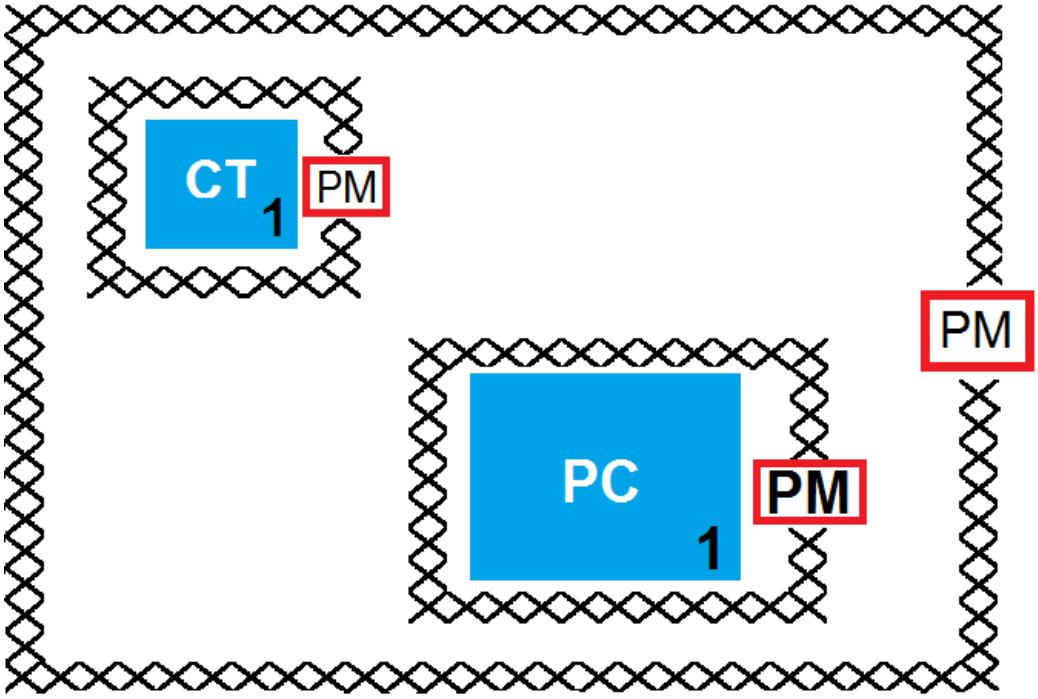



Figura 3: Despliegue de seguridad en un Puesto de Mando

En la Figura 3 el conjunto del CT y del PC estaría protegido por la Policía Militar, en la entrada con un piquete, rodeado en su conjunto con alambre y con patrullas interiores. A su vez, cada centro estaría protegido por la Policía Militar.

Como se ha comprobado, la seguridad en la parte interior del CT y del PC es alta. Esta parte sería la única en la cual el sistema viaja a través de cable UTP sin ser cifrado, esta extensión de terreno sería como máximo de 150 metros. Los servicios con los cuales se dota a un puesto de mando en el tramo entre el Centro de Transmisiones y el propio Puesto de Mando irían todos en ese trayecto sin cifrar, siendo encargados de su seguridad el personal de la Policía Militar destinada a tal efecto.

2. Del Centro de Transmisiones a otro Centro de transmisiones: Esta parte abarcaría una distancia de entre 10 km y los que fuesen necesarios para enlazar, por ejemplo, una base militar en Afganistán con Territorio Nacional. Para enlazar los puestos de mando existirían las siguientes opciones:

| ***ENLACE*** | ***SEGURIDAD*** |
|---|---|
| Rioja IP | Cifrador CM 109-IP |
| Satélite | Cifrador Epicom 430-C |
| | Cifrador Epicom 430-S |
| Red Conjunta de Telecomunicaciones | Confidencial |

Tabla 3. Enlaces entre Centros de Transmisiones.

En este trayecto la seguridad a la información sería dada por los distintos cifradores (tabla 3) de las estaciones encargadas del envío de información.

Como se ha podido constatar existen dos maneras diferentes de dar seguridad a la información. La primera sería una seguridad física proporcionada por personal de la Policía Militar, y la segunda la proporcionada por los cifradores de las diferentes estaciones existentes. Este punto tiene gran relevancia y debe entenderse. La principal baza con la que cuenta la VoIP en cuanto a seguridad no es la que le otorga el programa que se esté usando para la explotación de la VoIP sino las diferentes estaciones que se usan para el transporte de esa información y su sistema de seguridad. En la actualidad habría dos maneras distintas de ejecutar este transporte de la comunicación con dos sistemas de seguridad diferentes en cuanto a la encriptación y cifrado empleado.

Los dos potenciales puntos de ataque contra el sistema serían:

1. Introduciendo a una persona dentro del Centro de Transmisiones o dentro del Puesto de Mando que se conecte con su ordenador directamente a un switch y entre en el servidor. El riesgo de esta primera amenaza sería muy bajo ya que debería vulnerar toda la seguridad física de la Policía Militar y entrar dentro de uno de los dos puntos más protegidos de toda la maniobra. En el caso de lograr la realización de este ataque no sería un objetivo rentable entrar en el sistema de comunicaciones ya que si consigue entrar en el Puesto de Mando ha conseguido “neutralizar” toda la fuerza que lo defiende y al personal que trabaja en él

inclusive a los mandos que dirigen la operación. Si se eliminan estos mandos, dejaría de existir el flujo de información que captar.

2. El posible segundo ataque sería cuando la información ha salido de un Centro de Transmisiones y es transportada hacia otro Centro de Transmisiones en el cual exista otro Puesto de Mando. En este punto se debe tener en cuenta que la red usada para la explotación de los servicios de VoIP es aislada. Por ello la seguridad va enfocada contra medios de guerra electrónica en vez de la protección convencional que tienen los equipos usados en la vida civil, tales como los que se pueden encontrar en una casa o una empresa. De hecho ninguna de las dos centrales recibe actualizaciones de seguridad contra posibles ataques provenientes de internet ya que en ningún caso estos equipos militares se conectarán a dicha red. Los únicos medios que reciben este tipo de actualizaciones contra ataques serían los medios encargados de cifrar la información para su transporte. Debido a que la información referente a los cifradores no forma parte del trabajo, si se quiere ampliar la información sobre dichos cifradores, se puede recurrir a los anexos correspondientes.

### 3.3.3 Gestión de las centrales

Este apartado tiene como objetivo mostrar las diferencias entre la gestión de una y otra central mostrando las ventajas e inconvenientes de cada manera de ser gestionada y preparada para dar servicio.

Antes de profundizar en la gestión de las centrales se debe tener en cuenta que el BT II da servicio al Cuartel General de la Fuerza Ligera (CGFUL), este cuartel general se encarga de controlar y coordinar la maniobra de las tres brigadas ligeras con las que cuenta el Ejército Español. Desde este cuartel general se controlan unos 9.000 hombres teniendo en cuenta las brigadas y todos los apoyos necesarios para el cumplimiento de la misión. La envergadura e importancia que tiene el trabajo de dicho batallón para dar enlace al cuartel general con las tres brigadas es enorme, por ejemplo, en las últimas maniobras, las “Dragón”, el CGFUL desplegó en el campo de maniobras situado en Toledo y fue enlazado con el puesto de mando de la Brigada de Infantería Ligera Aerotransportable “Galicia VII” con sede en Figueirido (Pontevedra), con la Brigada “Rey Alfonso XIII” II de la Legión con sede en Viator (Almería), y con la Brigada Paracaidista “Almogávares” VI con sede en Paracuellos del Jarama (Madrid). Claramente sin el servicio del BT II estas maniobras no habrían sido posibles dada la complejidad del enlace.

El procedimiento seguido por el CGFUL al pedir apoyo al BT II sería el siguiente:

1. El CGFUL decide realizar un ejercicio durante un tiempo determinado en cualquier punto del Territorio Nacional (TN).
2. El CGFUL pide apoyo al BT II para que este último les dé servicio en base a una serie de características, en concreto para el ejercicio “Dragón” fueron desplegados por la sección de RBA de la compañía de puesto de mando alrededor de 140 teléfonos de VoIP gestionados por 3 suboficiales con el apoyo de la tropa.

Ante el volumen de trabajo la gestión debe ser lo más eficiente posible tanto en su despliegue como en la solución de los posible problemas que puedan surgir.

3. Una vez haya recibido el BT II la petición del apoyo la compañía de puesto de mando distribuye el trabajo en cuanto a los nodos SIMACET pedidos, las radios necesarias y los servicios de VoIP que sean necesarios.

En este punto comienzan las diferencias entre la configuración de una central de VoIP Asterisk y una central de VoIP de Call Manager.

- Asterisk:
  1. Lo primero que se debe realizar es la creación del servidor. Dicho servidor se puede crear en cualquier ordenador para sobre ese sistema operativo crear el servidor.
  2. Una vez creado el servidor el gestor debe crear la extensión de los números de teléfono, desde el General hasta el último soldado que lo utilice.
  3. Asociar cada extensión a una dirección IP determinada de cada teléfono.
  4. Realización de los troncales con el resto de PC.
  5. Categorizar cada teléfono.

Todo este proceso se ha llevado semanas antes de las maniobras, es decir, antes del despliegue del PC en el campo la sección de RBA ha desarrollado todo el trabajo.

En el momento del despliegue en el campo simplemente se debería realizar todo el montaje de la red y empezar su explotación.

- Call Manager:

La principal característica de Call Manager es que sólo puede ser configurado para unas maniobras de tal envergadura por el Centro de Gestión de Sistemas (CGES) con sede en Madrid a través de un enlace Satélite. Dicha configuración es cargada directamente sobre un router especial de la empresa Cisco que ha sido comprado previamente con un número de licencias determinado. La central Call Manager sería ese router con el servidor cargado en su interior. El proceso de configuración del servidor sería sencillo, el BT II haría la petición y sería el CGES el encargado de toda la gestión. Una vez configurado todo por parte del CGES el BT II sólo debería comprobar el correcto diseño de la red y su posterior despliegue en el campo.

Comparación de Gestión

A priori la gestión de Call Manager sería mucho más sencilla que la gestión de Asterisk ya que sería un trabajo que no realizaría la unidad y por tanto no sería responsabilidad suya. Además se descargaría todo ese volumen de trabajo a la sección, pero se deben tener en cuenta los siguientes aspectos en esta comparación:

1. Si la RBA es reemplazada por la VoIP en el futuro y el CGES debe encargarse de toda la gestión de las centrales Call Manager del Ejército, el CGES será claramente un embudo. Esto es debido a que hoy en día sólo unas pocas unidades disponen de este sistema pero si se hace efectivo en el futuro y el CGES debe realizar todas las configuraciones el volumen de trabajo de este departamento será demasiado alto. Además restaría importancia a los Batallones de Transmisiones ya que serían simples montadores de la red quitándole todo el conocimiento técnico actual que les caracteriza.
2. Se debe tener en cuenta que cualquier error aparecido durante la maniobra en cualquiera de las centrales de VoIP debe ser solventado de la manera más rápida posible debido a las consecuencias que puede tener la falta de enlace en un momento determinado con una unidad que se encuentra en combate desde el punto de vista de los apoyos que pueda necesitar o simplemente la situación del enemigo en un contraataque del mismo. Por ello la gestión integra de las centrales de VoIP debe encontrarse en el mismo lugar de la explotación de dicho servicio. Por ejemplo con Asterisk si aparece un problema puede solucionarse en ese mismo instante y es más fácil de coordinar por un jefe único en el mismo Puesto de Mando ya que la gestión de la central se realiza en el Centro de Transmisiones adyacente al Puesto de Mando. Sin embargo en caso de aparecer un error con Call Manager primero se deberá asegurar el enlace satélite para la gestión de la central por parte del

CGES y posteriormente coordinar con dicho departamento a kilómetros de distancia la solución del problema.

3. Desde el punto de vista de la prevención de los errores, las transmisiones tienden a tener por duplicado sus sistemas para evitar los problemas que conlleva la pérdida de enlace. En el caso de las centrales de VoIP se trata de la manera siguiente:
    - Asterisk: En el caso de que caiga esta central, al ser simplemente una virtualización que funciona en prácticamente cualquier ordenador, la sección de VoIP llevaría varios ordenadores por si falla alguno de ellos y el sistema virtualizado lo lleva clonado, por tanto, si falla solo se debería encender otro ordenador con el servidor de Asterisk clonado y enchufar el switch o router principal a este nuevo ordenador para que todo vuelva a funcionar en cuestión de minutos.
    - Call Manager: Como ya se ha explicado el servidor iría integrado en un router de la empresa Cisco, este router ha sido configurado antes de las maniobras por el CGES. Si este router por cualquier motivo deja de funcionar, la red que forma desaparecería. La solución sería tener varios router de la empresa Cisco configurados por si aparece fallo en alguno de ellos durante su explotación. De esta manera se conseguiría sobrecargar con más trabajo al CGES creando un embudo aún más grande al tener que configurar más router que los que realmente se van a utilizar por si los primeros fallan y además se tendría el problema del presupuesto.

Número aproximado de centrales Call Manager a configurar por el CGES:

| **Tipo de unidad** | **Nº aproximado de unidades tipo** | **Nº aproximado de centrales por unidad tipo** | **Total** |
|---|---|---|---|
| Compañías de transmisiones de las brigadas | 7 | 2 | 9 |
| Unidades de transmisiones en apoyo a regimientos de artillería antiaérea | 2 | 2 | 4 |
| Unidades de transmisiones de las plazas de Ceuta, Melilla y el Mando de Canarias | 3 | 2 | 5 |
| Regimientos de transmisiones | 2 | 5 | 7 |
| | | **TOTAL** | 25 |

Tabla 4. Número aproximado de Centrales Call Manager en el Ejército

Como se puede observar en la tabla 4 con aproximadamente 25 centrales Call Manager y con un número máximo de 475 teléfonos configurables por central según el router cisco 3900 series en dotación en el Ejército daría un número de 11.875 teléfonos a configurar en un pico de trabajo. Siendo no viable con un único departamento la configuración total de las centrales en un corto periodo de tiempo.

### 3.3.4 Servicios y compatibilidades

El objetivo de este punto es comparar los servicios que puede dar cada una de las centrales así como la compatibilidad de las mismas con diferentes modelos de diferentes proveedores.

#### Asterisk

La central Asterisk es una central de código abierto, partiendo de esta premisa y sumándole el protocolo SIP como protocolo usado para la comunicación con los diferentes terminales, el Ejército dispone de una central polivalente con la cual es difícil que encuentre problemas de compatibilidad con las diferentes marcas del mercado civil. El único requisito para que fuese compatible con un determinado terminal sería que el códec usado por dicho terminal estuviese dentro de la pila de códec de la central Asterisk. La pila de códec compatibles con la central serían [2]:

- G.711: bit-rate de 64 Kbps.
- G.722: bit-rate de 64 Kbps.
- G.723.1: bit-rate de 5,3 o 6,4 Kbps.
- G.728: bit-rate de 16 Kbps.
- G.729: bit-rate de 8 o 13 Kbps.
- ILBC: bit-rate de 13 Kbps.
- GSM: bit-rate de 8 Kbps.

Desde el punto de vista de los servicios el BT II no ha encontrado un número máximo de terminales. Ha sido probada hasta con 150 teléfonos, siendo este número el máximo de los teléfonos necesarios usados por un puesto de mando de entidad división.

#### Call Manager

Esta central dará más problemas en cuanto a la compatibilidad ya que no sólo depende de los códec sino que también depende del sistema operativo instalado en el router. Dependiendo del sistema operativo instalado se tendrá un número determinado de licencias (número máximo de teléfonos que se pueden usar). Además, dependiendo de la versión del sistema operativo habrá una serie de modelos compatibles que se podrán usar mientras que otros modelos no serán configurables con el router en cuestión. Por ejemplo, un router X lleva asociado según el presupuesto empleado en su compra un número determinado de teléfonos del modelo Y, cuanto

más dinero se emplee en su compra, mayor número de teléfonos del modelo Y se podrán usar. Al igual que existen teléfonos del modelo Y existen multitud de modelos diferentes que pueden no ser compatibles y ser inservibles con el modelo del router X.

### 3.3.5 Presupuestos

Este último apartado ha sido enfocado a la creación de un presupuesto aproximado del dinero que sería necesario para la puesta en marcha de un sistema de VoIP para una unidad tipo brigada la cual sería apoyada por una compañía de transmisiones. De esta manera se quiere comprobar el rendimiento que se pudiera recibir del presupuesto en la puesta en marcha de una y otra central. Los datos sacados para la realización de dicho presupuesto (tabla 5) han sido obtenidos en caso de los teléfonos, ordenador, y tarjetas de integración necesarios de la página web de Amazon y en caso del router Cisco 3900 series de la sección de logística del BT II. Todo el material expuesto se encontraría en la actualidad en dotación en dicho batallón y las prestaciones de los terminales que dan servicio con cada una de las centrales serían similares:

| **Asterisk** | | |
|---|---|---|
| ***Producto*** | ***Servicio*** | ***Precio*** |
| Gxp1620 IP | Llamadas | 43,79 € |
| Grandstream GXW4108 Analog FXO Gateway 8 bocas | Tarjeta para la integración de la red con una red analógica | 246 € |
| Grandstream GXW4008 Analog FXS Gateway 8 bocas | Tarjeta para la integración de la red con una red analógica | 165 € |
| Hacer Aspire 573-35J5 | Ordenador sobre el que crear y gestionar el servidor de Asterisk. | 344,85 € |
| Total | | 756 € |
| | | Más 43,79 por el número de teléfonos necesario |

| **Cisco** | | |
|---|---|---|
| ***Producto*** | ***Servicio*** | ***Precio*** |
| Cisco 7841 | Llamadas | 186,64 € |
| Router cisco 3900 series | Central de Call Manager con 4 tarjetas FXO y 4 tarjetas FXS integradas.<br>Capacidad para 475 teléfonos Cisco. | 4,500 € |
| Total | | 4.686,64 € |
| | | Más 186,64 por el número de teléfonos necesario |

Tabla 5. Presupuesto para la obtención de las centrales de VoIP

Para una unidad de tipo brigada como podría ser la Brigada “Rey Alfonso XIII” II de la Legión se ha creado un presupuesto aproximado (tabla 6) para una de sus maniobras, con la formación de dos puestos de mando y una dotación de personal con necesidad de teléfonos IP de 24 personas se necesitaría la siguiente cantidad de recursos:

| **Asterisk** | Teléfonos IP | Central | Tarjeta FXO | Tarjeta FXS |
|---|---|---|---|---|
| Cantidad | 24 + 5 de reserva | 1 + 1 de reserva | 1 + 1 de reserva | 1 + 1 de reserva |
| Presupuesto | 1.268,91 € | 689,70 € | 492 € | 330 € |
| **Total necesario** | **2.780,61 €** | | | |

| **Call Manager** | Teléfonos IP | Central |
|---|---|---|
| Cantidad | 24 + 5 de reserva | 1 + 1 de reserva |
| Presupuesto | 5.412,56 € | 9.000 € |
| **Total** | **14 412,56 €** | |

Tabla 6: Presupuesto necesario para un sistema de VoIP en una unidad tipo brigada.

# 4 Comparación de los sistemas de VoIP

Este último capítulo del trabajo de fin de grado ha sido enfocado en la comparación de los sistemas de VoIP. Para ello se recogerán los resultados obtenidos en las pruebas del capítulo anterior y se someterán a un juicio crítico.

## 4.1 Ancho de banda

Se ha comprobado que ambas centrales tendrían un consumo de ancho de banda similar durante la transmisión de la información. Este ancho de banda sería de 100 Kbps, superior al esperado de manera teórica, ya que debería ser menor debido al códec usado para las pruebas de campo, el códec G711ulaw que teóricamente ocupa un ancho de banda de 64 Kbps. El aumento en el ancho de banda es debido a los protocolos que ambas centrales utilizan para la comunicación entre los terminales que se encarga del inicio, establecimiento, mantenimiento y finalización de la llamada. Dentro de la investigación llevada a cabo se ha comprobado que la diferencia entre una y otra central vendrá marcada por los protocolos que utiliza, por ello el estudio dentro de este ámbito es enfocado a los protocolos.

La central Asterisk utiliza el protocolo SIP para la comunicación con sus terminales y el modo de codificación de la voz que utiliza sería el modo CBR (tasa de bits constante), es decir, desde el inicio hasta el fin de la llamada ocuparía 100 Kbps estuvieran o no los usuarios transmitiendo la información

La central Call Manager utiliza el protocolo SCCP para la comunicación con sus terminales y el modo de codificación de la voz utilizado es el VBR (tasa de bits variable), es decir, adapta el ancho de banda ocupado en la transmisión a los datos que se envían entre los terminales debido a la información enviada por los usuarios. Este modo de codificación ocuparía 100 Kbps mientras los usuarios estuvieran hablando y aproximadamente 50 Kbps durante los silencios de la conversación.

A la vista de los resultados obtenidos, la central Call Manager utiliza el ancho de banda de una manera más eficiente que la central Asterisk.

## 4.2 Seguridad

En este aspecto los resultados que se han obtenido difieren de lo esperado. Pese a que la seguridad es uno de los puntos de mayor relevancia en cuanto al trato de información, no se debe exigir ningún tipo de medida de seguridad a ninguna de las dos centrales ya que el Ejército utiliza una serie de medios (cifradores) para tal efecto. El Ejército utiliza un sistema de seguridad en el cual asegurando un alto nivel de seguridad en el sistema de transmisión garantiza que los datos no pueden ser descifrados. Por tanto, ambas centrales cumplen los requisitos de seguridad necesarios para su puesta en servicio en el Ejército de Tierra.

## 4.3 Gestión

Si se tiene en cuenta el estudio que se ha realizado en cuanto a los diferentes sistemas de gestión y solución de errores de cada una de las centrales, se llega a las siguientes conclusiones:

- El CGES sería sin lugar a dudas un embudo al tener que realizar todas las configuraciones de la central Call Manager de cada una de las unidades del Ejército. En la actualidad al no estar este sistema implantado a nivel Ejército, sino que sólo está en servicio en las unidades independientes del arma de transmisiones salvo algunas excepciones, el CGES no tiene gran volumen de trabajo, pero como se ha demostrado si la VoIP sustituyera al sistema de la RBA existente en la actualidad y fuese la central Call Manager la elegida, el volumen de trabajo sobrepasaría lo esperado y el CGES sería un punto conflictivo en la puesta en marcha de dicho sistema.
- Debido a la solución de los posibles errores Asterisk daría mayor velocidad en la solución de los mismos debido a que cualquier problema ocurrido durante la maniobra sería solucionado in situ sin necesidad de contactar con una unidad externa, además no se necesitaría el enlace satélite para la reconfiguración de la central en caso de que esta o cualquiera de los terminales fallase.

Por ello, en vista de las dificultades de gestión y solución de errores de la central Call Manager en comparación con la central Asterisk, es la central Asterisk la que mejor rendimiento en cuanto a gestión otorga.

### 4.4 Servicios y compatibilidades

Estas pruebas de campo fueron enfocadas a averiguar qué central tendría mayor compatibilidad con los diferentes modelos existentes en el mercado así como la cantidad de líneas de teléfono que pudiera otorgar cada una de las centrales.

- La central Asterisk ha sido la que ha obtenido mejores resultados. Esto es debido a que dicha central es de código abierto y siempre dará más facilidades a la hora de utilizar teléfonos de distintas marcas y modelos. Además el número máximo de teléfonos que se podrían usar como máximo superaría el número de teléfonos necesarios para los ejercicios y maniobras de la unidad.
- La central Call Manager será la central que dé más problemas en cuando a la compatibilidad ya que no sólo no será compatible con diferentes marcas civiles, sino que también tendrá problemas con los diferentes modelos dentro de la marca Cisco debido a la versión del software que tenga instalada dicha central, ya que cada versión del software lleva asociados una determinada gama de modelos de la marca Cisco. El número de líneas de teléfono de las cuales se dispondrá dependerá de la cantidad de presupuesto del que se disponga, a mayor presupuesto mayor número de líneas de teléfono.

En vista de los resultados La central Asterisk respondería con mayor eficacia en cuanto a compatibilidad con los diferentes terminales existentes en el mercado. En cuanto a los servicios se debe realizar una comparativa del presupuesto usado para poder discernir sobre qué central otorga los servicios de una manera óptima.

### 4.5 Presupuesto

La importancia de este último apartado es alta debido a que uno de los propósitos del Ejército de Tierra es optimizar el uso del presupuesto para dotar a sus unidades con el mejor material posible utilizando para ello la menor cantidad de presupuesto necesario. Por ello y en vista de los resultados obtenidos en el presupuesto necesario obtenido de manera aproximada para dotar a una brigada del material necesario para el funcionamiento de la misma con sistemas de VoIP, de nuevo es la central Asterisk con una diferencia de presupuesto de 11.631,92 € la que mayor eficacia tendría en el gasto de presupuesto.

## 4.6 Elección de uno de los sistemas de VoIP

Teniendo en cuenta el resultado de la comparativa entre las dos centrales de VoIP, siendo estos resultados favorables en 3 de las 5 pruebas realizadas siendo una de las mismas nula teniendo la misma reacción en ambas centrales, la central elegida para la puesta en marcha de un sistema de VoIP sería la central Asterisk de Digium.

# 5 Conclusiones y líneas futuras.

Para finalizar la presente memoria se debe extraer una serie de conclusiones a raíz del trabajo realizado y exponer las líneas futuras de investigación las cuales, debido a la limitación de tiempo, contenido y temario estudiado, no han podido abarcarse pero deben ser objeto de estudio para un análisis e implementación futuro.

## 5.1 Conclusiones

Dentro de este apartado se van a exponer las conclusiones obtenidas del trabajo fin de grado, las cuales han sido extraídas de la realización de la investigación así como de cada una de las pruebas de campo realizadas.

- Se ha hecho evidente que la importancia de la VoIP en el Ejército de Tierra es muy alta, debido a la imperiosa necesidad de actualización que tienen los equipos actuales que conforman la RBA con el fin de unificar todos los servicios de voz en un puesto de mando así como la facilidad en la configuración, gestión y solución de problemas en dichos equipos.
- La elección de una de estas centrales de VoIP es urgente, no solo debido a la mencionada necesidad de modernización de los sistemas de comunicaciones si no también debido a la obligación de evitar el desperdicio de recursos económicos, materiales y de personal en el Ejército.
- La elección de una de estas centrales debe ser fundamentada y basada en pruebas de campo debido a que el servicio de una central de VoIP dentro del Ejército es diferente a la vida civil, por tanto hay que ser consciente de que las distintas circunstancias a las que se deben someter dichas centrales son más exigentes, para ajustarlas a los condicionantes operativos y técnicos actuales.
- La importancia en el ancho de banda que ocupa una central no sólo radica en el códec utilizado, sino también en gran medida en los protocolos que aseguran el inicio, establecimiento, y fin de la llamada. Ha de darse preferencia a aquellos modos de codificación que al igual que el modo VBR ajustan el ancho de banda ocupado a la cantidad de información transmitida. Es de vital importancia, llegados a este punto, que dentro de las características que debe tener una central de VoIP este la escalabilidad. Es decir, con estos sistemas se debe ser capaz de dar servicio a cuantos usuarios se necesite, no sólo a un

pequeño puesto de mando sino también a un cuartel general de división según necesidades de la operación. También se ha de tener en cuenta la importancia de la flexibilidad en estos equipos, ya que una misma central de VoIP debe estar preparada para dar servicio en los diferentes puestos de mando con las distintas configuraciones que este trabajo pudiera necesitar.

- La seguridad es otro de los puntos importantes dentro de un sistema de información militar. Como se ha comprobado, la seguridad no solo se garantiza gracias al sistema de VoIP a través de sus protocolos sino que también y en mayor medida se debe primeramente a la seguridad que es aportada físicamente en los puestos de mando a través de personal militar y a la seguridad en la transmisión de información que aportan aquellos medios y estaciones existentes para tal efecto. Siendo más crítica la seguridad dada por estos últimos medios nombrados, los cifradores.
- La gestión es sin duda el punto con mayor relevancia desde el punto de vista de las unidades de transmisiones. La gestión no debe ser centralizada en un único departamento o entidad debido a las dificultades que dicho tipo de gestión conlleva en la configuración de los equipos así como en la solución de los problemas que puedan aparecer durante las operaciones además de la dependencia del enlace satélite para la solución de los mismos. La configuración debe ser realizada in situ por el personal encargado de su despliegue así como accesible en cualquier momento del despliegue.
- La compatibilidad debe ser total y absoluta tanto con los medios actuales en dotación como con las futuras adquisiciones de sistemas de VoIP. La mejor opción para este tipo de compatibilidad sería una central de código abierto ya que ofrecerá una compatibilidad mayor con los diferentes terminales del mercado. El punto más relevante en este aspecto sería la importancia de que el Ejército no se comprometiera en la adquisición del material con una determinada marca en concreto debido al potencial monopolio y dependencia que existiría en ese caso con dicha entidad, así como la dificultad de la reposición o actualización de los materiales en caso de la desaparición o rescisión del contrato con la misma.

## 5.2 Líneas futuras

Estas líneas futuras de trabajo van encaminadas al estudio de la mejora del sistema de VoIP español visto como el futuro de las telecomunicaciones militares, el cual se encuentra en un estado embrionario debido a su reciente puesta en marcha. Las líneas futuras de investigación podrán ser las siguientes:

- Para la realización de este trabajo no se ha tenido en cuenta la **interoperabilidad** de las centrales de VoIP con el resto de **Ejércitos de los países aliados**, así como las diferentes alianzas contraídas por España con las **Organizaciones Internacionales**, por ello una futura línea de estudio sería la interoperabilidad de los sistemas de VoIP nacionales con los diferentes medios de transmisiones extranjeros.
- Al encontrarse en los momentos iniciales de implantación, la VoIP no cuenta con un sistema de QoS, por ello el Ejército se encuentra funcionando hasta ahora sin este sistema. Un posible **estudio** futuro sería el desarrollo de un **sistema de QoS en los puestos de mando**.
- La principal desventaja de la central Call Manager sería el problema de gestión en cuanto a la configuración de los equipos, por tanto se podría desarrollar un estudio para la configuración de dichos router por parte de las unidades. Para ello habría que desarrollar un análisis de las **políticas y protocolos de seguridad del CGES**.

En resumen, la adopción de sistemas de VoIP presenta innumerables ventajas a la vez que presenta nuevos retos a los que las FAS deben afrontarse como parte del objetivo de modernización e innovación que establece el ministerio de Defensa: "*La modernización es imprescindible para dotar a las Fuerzas Armadas de los medios precisos, con el nivel óptimo de operatividad y seguridad. Para ello, se requiere un gran esfuerzo y equilibrio entre inversión y necesidades* ".

## Bibliografía

1. Dr. Ing. José Joskowicz; Conceptos básicos de telefonía, **2015.**
2. Tte. D. Antonio García-Matres Bellod; Apuntes curso VoIP: Hardware y Software basado en centralita Trixbox 2.8.0.3.
3. Comandante Don Juan Manuel Lopera López; Transmisión de datos, Volumen II, Transmisión de datos multimedia, **2016**.
4. Dr. Juan Carlos Corrales Muñoz y Dr. Álvaro Rendón Gallón, Universidad de Cauca, Facultad de Ingeniería Electrónica y Telecomunicaciones Departamento de Telemática; Sistemas de Conmutación, Telefonía IP, Voz sobre IP (VoIP), Conceptos y arquitectura. **2011.**
5. Cisco. Calidad del servicio para Voz sobre IP.

## Listado de Figuras



## Listado de tablas

## Listado de anexos

Anexo A Protocolos de transmisión por la red

# TCP/IP

Junio 2014

## ¿Qué significa TCP/IP?

**TCP/IP** es un conjunto de protocolos. La sigla TCP/IP significa **"Protocolo de control de transmisión/Protocolo de Internet"** y se pronuncia "T-C-P-I-P". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- dividir mensajes en paquetes;
- usar un sistema de direcciones;
- enrutar datos por la red;
- detectar errores en las transmisiones de datos.

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental.

## La diferencia entre estándar e implementación

En general, TCP/IP relaciona dos nociones:

- la noción de **estándar**: TCP/IP representa la manera en la que se realizan las comunicaciones en una red;
- la noción de **implementación**: la designación TCP/IP generalmente se extiende a software basado en el protocolo TCP/IP. En realidad, TCP/IP es un modelo cuya aplicación de red utilizan los desarrolladores. Las aplicaciones son, por lo tanto, implementaciones del protocolo TCP/IP.

## TCP/IP es un modelo de capas

Para poder aplicar el modelo TCP/IP en cualquier equipo, es decir, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha dividido en diversos módulos. Cada uno de éstos realiza una tarea específica. Además, estos módulos realizan sus tareas uno

después del otro en un orden específico, es decir que existe un sistema estratificado. Ésta es la razón por la cual se habla de **modelo de capas**.

El término capa se utiliza para reflejar el hecho de que los datos que viajan por la red atraviesan distintos **niveles de protocolos**. Por lo tanto, cada capa procesa sucesivamente los datos (paquetes de información) que circulan por la red, les agrega un elemento de información (llamado *encabezado*) y los envía a la capa siguiente.

El modelo TCP/IP es muy similar al modelo OSI (modelo de 7 capas) que fue desarrollado por la Organización Internacional para la Estandarización (ISO) para estandarizar las comunicaciones entre equipos.

## Presentación del modelo OSI

OSI significa *Interconexión de sistemas abiertos*. Este modelo fue establecido por ISO para implementar un estándar de comunicación entre equipos de una red, esto es, las reglas que administran la comunicación entre equipos. De hecho, cuando surgieron las redes,cada fabricante contaba con su propio sistema (hablamos de un sistema patentado), con lo cual coexistían diversas redes incompatibles. Por esta razón, fue necesario establecer un estándar.

La función del modelo OSI es estandarizar la comunicación entre equipos para que diferentes fabricantes puedan desarrollar productos (software o hardware) compatibles (siempre y cuando sigan estrictamente el modelo OSI).

## La importancia de un sistema de capas

El objetivo de un sistema en capas es dividir el problema en diferentes partes (las capas), de acuerdo con su nivel de abstracción.

Cada capa del modelo se comunica con un nivel adyacente (superior o inferior). Por lo tanto, cada capa utiliza los servicios de las capas inferiores y se los proporciona a la capa superior.

## El modelo OSI

El modelo OSI es un modelo que comprende 7 capas, mientras que el modelo TCP/IP tiene sólo 4. En realidad, el modelo TCP/IP se desarrolló casi a la par que el modelo OSI. Es por ello que está influenciado por éste, pero no sigue todas las especificaciones del modelo OSI. Las capas del modelo OSI son las siguientes:

| Nivel | Modelo antiguo | Modelo nuevo |
|---|---|---|
| Nivel 7 | | |
| Nivel 6 | | |
| Nivel 5 | | |
| Nivel 4 | | |
| Nivel 3 | | |

| Nivel 2 |
| --- |
| Nivel 1 |

- **La capa física** define la manera en la que los datos se convierten físicamente en señales digitales en los medios de comunicación (pulsos eléctricos, modulación de luz, etc.).
- **La capa de enlace de datos** define la interfaz con la tarjeta de interfaz de red y cómo se comparte el medio de transmisión.
- **La capa de red** permite administrar las direcciones y el enrutamiento de datos, es decir, su ruta a través de la red.
- **La capa de transporte** se encarga del transporte de datos, su división en paquetes y la administración de potenciales errores de transmisión.
- **La capa de sesión** define el inicio y la finalización de las sesiones de comunicación entre los equipos de la red.
- **La capa de presentación** define el formato de los datos que maneja la capa de aplicación (su representación y, potencialmente, su compresión y cifrado) independientemente del sistema.
- **La capa de aplicación** le brinda aplicaciones a la interfaz. Por lo tanto, es el nivel más cercano a los usuarios, administrado directamente por el software.

## El modelo TCP/IP

El modelo TCP/IP, influenciado por el modelo OSI, también utiliza el enfoque modular (utiliza módulos o capas), pero sólo contiene cuatro:

| Capa de aplicación |
| --- |
| Capa de acceso a la red |

Como puede apreciarse, las capas del modelo TCP/IP tienen tareas mucho más diversas que las del modelo OSI, considerando que ciertas capas del modelo TCP/IP se corresponden con varios niveles del modelo OSI.

Las funciones de las diferentes capas son las siguientes:

- **capa de acceso a la red**: especifica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado;
- **capa de Internet**: es responsable de proporcionar el paquete de datos (datagrama);
- **capa de transporte**: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión;
- **capa de aplicación**: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

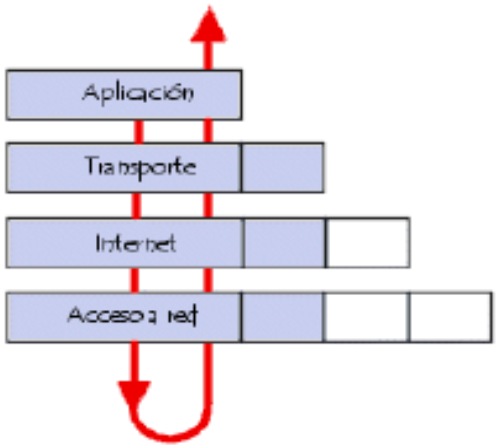
A continuación se indican los principales protocolos que comprenden el conjunto TCP/IP:

Aplicaciones de red TCP o UDP IP, ARP, RARP FTS, FDDI, PPP, Ethernet, Red de anillos

## Encapsulación de datos

Durante una transmisión, los datos cruzan cada una de las capas en el nivel del equipo

remitente. En cada capa, se le agrega información al paquete de datos. Esto se llama **encabezado**, es decir, una recopilación de información que garantiza la transmisión. En el nivel del equipo receptor, cuando se atraviesa cada capa, el encabezado se lee y después se elimina. Entonces, cuando se recibe, el mensaje se encuentra en su estado original.




En cada nivel, el paquete de datos cambia su aspecto porque se le agrega un encabezado. Por lo tanto, las designaciones cambian según las capas:

- el paquete de datos se denomina **mensaje** en el nivel de la capa de aplicación;
- el mensaje después se encapsula en forma de **segmento** en la capa de transporte;
- una vez que se encapsula el segmento en la capa de Internet, toma el nombre de **datagrama**;
- finalmente, se habla de **trama** en el nivel de capa de acceso a la red.

## Capa de acceso a la red

La capa de acceso a la red es la primera capa de la pila TCP/IP. Ofrece la capacidad de acceder a cualquier red física, es decir, brinda los recursos que se deben implementar para transmitir datos a través de la red.
Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una red de área local (Red en anillo, Ethernet, FDDI), conectada mediante línea telefónica u otro tipo de conexión a una red. Trata los siguientes conceptos:

- enrutamiento de datos por la conexión;
- coordinación de la transmisión de datos (sincronización);
- formato de datos;
- conversión de señal (análoga/digital);
- detección de errores a su llegada.
- ...

Afortunadamente, todas estas especificaciones son invisibles al ojo del usuario, ya que en realidad es el sistema operativo el que realiza estas tareas, mientras los drivers de hardware permiten la conexión a la red (por ejemplo, el driver de la tarjeta de red).

## La capa de Internet

La capa de Internet es la capa "más importante" (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP.
Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben.

La capa de Internet contiene 5 protocolos:

- el protocolo IP;
- el protocolo ARP;
- el protocolo ICMP;
- el protocolo RARP;
- el protocolo IGMP.

Los primeros tres protocolos son los más importantes para esta capa.

## La capa de transporte

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones.
De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, etc. Además, el nombre de la aplicación puede variar de sistema en sistema. Es por ello que se ha implementado un sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se denominan puertos.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores). Estos dos protocolos son los siguientes:

- TCP, un protocolo orientado a conexión que brinda detección de errores;
- UDP, un protocolo no orientado a conexión en el que la detección de errores es obsoleta.

## La capa de aplicación

La capa de aplicación se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores.
Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo. Se pueden clasificar según los servicios que brindan:

- servicios de administración de archivos e impresión (transferencia);
- servicios de conexión a la red;
- servicios de conexión remota;
- diversas utilidades de Internet.

Anexo B Cifrador CM 109IP

# CM109IP
## IP CRYPTO DEVICE

## DESCRIPTION

CM109IP is an IP encryption device that enables the creation of a "Virtual Private Network". A VPN is a network that features secure nodes by which those communications, using an insecure IP public network, take place. CM109IP is based upon the IP protocols, and it generates a VPN according to IETF IPSEC specifications fitted to use military algorithms. CM109IP uses a completely new multiprocessor architecture, appointed to increase performance and avoid security problems. The encryption procedure also includes the protected LAN addresses.

Encryption is performed at the 3rd IP layer (IP-layer) and thus all communications are carried out on higher protocols (TCP/IP, UDP etc) and the relevant services (Mail, Telnet, FTP, etc.) are made secure.

A different key is used for each LAN with a different address.

Key uploading is made up by a mobile electronic transfer device (punched tape reader or fill gun). Keys and access lists can be centrally managed (through the management system KNMS109IP) by the IP network and by protected connections.

## MAIN FEATURES

- Communication protocols are implemented via software to allow easy upgrade of new functionalities (IP v.6)
- Selectable AUI or 100 base TX interface either on the red or on the black side
- Encryption algorithm on a removable dedicated module that allows it to be easily changed (with other standard or customisable algorithms)
- Modular interfaces structure with a general CPU sub-unit that supports the development of different interface formats (ex. WAN).

### Applications

- Secure connections between IP/Ethernet
- LAN on insecure public networks.

### Security services

- Data confidentiality (encryption/decryption)
- Authentication
- Data integrity
- Traffic flux confidentiality (IP address encryption).

### Algorithms

- NATO approved
- Nationally approved
- Customisable.

### Keys storage

- Key protection from possible main power failure
- Protection time: up to six months.


CM109IP
IP Crypto Device

### Security protocols

- IPSEC: IPSEC (RFC 2401) Architecture
- AH: Authentication Header (RFC 2402)
- ESP: Encapsulating Security Payload (RFC 2406) in tunnelling mode.

### Remote control channel

- Via IP encrypted network.

### Accesses control

- Anti tampering function
- Emergency deletion by a mechanical switch (also in case of turning off or main power failure).

### Logging

- Configuration operation system for the events
- System and security alarms.

### User interfaces

- Front panel (0screen, keypad).

### Communication protocols

- IP, ARP, ICMP
- TCP, UDP.

### Other features

- Built in Test Equipment (BITE)
- Access list
- Multicasting
- QoS (Quality of Services).

### Implementation functionalities

- VRRP (Virtual Router Redundancy Protocol)
- OSPF (Open Shortest Path First)
- GRE (Generic Routing Encapsulation)
- IPV.6.

### Network interfaces

- Red side and black side:
  - 10 Mbit/s AUI interface (IEEE 802.3);
  - 100BaseTX (UTP).

### EMI/EMC

- MIL-STD-461
- MIL-STD-462.

### TEMPEST

- AMSG-720B.

### Environmental conditions

- Operating temperature: from -10°C to +45°C
- Storage temperature: from -40°C to +70°C
- Relative humidity: 90% @ +45°C.

### Physical features

- Dimensions: 92H x 448L x 395D mm
- Weight: 13 kg.

### Power supply

- Input voltage: 115/220 Vac ± 15% 45-63 Hz, 21-60 Vdc
- Power: 60W max.

## Ancillary devices: FG101


FG101 is a mobile device used to store a maximum of 8 keys in compliance with the EUROCOM D/1 Crypto Supplement, or a maximum of 4 encrypted keys.

It is endowed with a battery that allows storage of the keys for up to one year.

- Line interface according to the EUROCOM D/1 Crypto Supplement
- Internal supply battery type: BA1372/U 6.75V-BA5372/U 6V.

### Physical data

- Dimensions: 75 x 150 x 45 mm (H x L x D)
- Weight: 0.6 kg.

## TR101


TR101 is a portable punched tape reader used to transfer the keys on tape in compliance with the EUROCOM D/1 Crypto Supplement.

It is endowed with an internal battery that has a duration of one year.

- Line interface in compliance with the EUROCOM D/1 Crypto Supplement
- Internal supply battery type: BA1372/U 6.75V-BA5372/U 6V.

### Physical data

- Dimensions: 60 x 150 x 45 mm (H x L x D)
- Weight: 0.7 kg.

.


Fuente : https://www.ia.nato.int/niapc/Product/CM-109-IP_134

Anexo C Cifrador EP-430 C

**JEFATURA DE APOYO LOGISTICO DE LA ARMADA**

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

C/. PIO XII, 83
28036 - MADRID

# PLIEGO DE PRESCRIPCIONES TÉCNICAS

## SUMINISTRO DE EQUIPOS DE CIFRA NACIONALES EPICOM EP- 430GN Y EP-430 C




Mayo 2014

## 1. INTRODUCCIÓN.

Este Pliego de Prescripciones Técnicas (PPT) establece los requisitos técnicos para la adquisición de cifradores de datos EP-430GN Y EP-430C, solicitados por el EMA (INFOSEC) en su mensaje AJEMA 15059 de 051102Z MAY 14 .

## 2. DESCRIPCIÓN DEL SUMINISTRO.

### Cifrador IP EP-430GN.

Cifrador para servicios de seguridad a las comunicaciones basadas en el protocolo TCP-IP.

Características generales:

- Nivel Físico: 10BaseT con posibilidad de instalar AUI.
- Nivel de enlace: Ethernet/IEEE 802.3.
- Recomposición de los datagramas fraccionados en su tránsito por la red.
- Operación transparente a todos los protocolos entre zonas rojas.
- Tráfico cifrado y encapsulado en datagramas UDP.
- CONFIDENCIALIDAD: Cifrado por suma módulo 2 con la serie cifrante. Algoritmo simétrico.
- IDENTIDAD USUARIOS: Cifrado de los datagarmas IP incluyendo la cabecera.
- INTEGRIDAD de los datos, utilizando mecanismos asociados al cifrado.
- AUENTICACION de origen y destino, utilizando propiedades del Sistema de Gestión de claves EPICOM.
- CONTROL DE ACCESO, mediante tarjeta electrónica grabada en el Centro de Gestión.
- Protecciones contra "replay" y otros ataques.

Protecciones:

-Borrado automático de claves en caso de apertura de la caja o mediante pulsador en panel frontal.
- Auditorías. Registro automático de alarmas y eventos significativos.
- Autenticación del software.
- Identidad del cifrador basada en un número de serie interno inviolable.
- Supervivencia de la red en caso de captura de las claves de un cifrador. Información de claves almacenada en cada cifrador debe ser UNICA en la red.
- Diseño TEMPEST.

Gestión de claves:

- Capacidad para 10 bancos de Claves, que permiten formar grupos cerrados de usuarios.
- Claves únicas e irrepetibles para cada datagrama IP.

- Claves de Asociación de Seguridad exclusivas para cada posible pareja de cifradores y diferentes cada vez que se establece la Asociación entre dos cifradores.

Carga de Claves:
-Manual, a través del teclado del teléfono asociado.
-Por medio de tarjeta electrónica
-Por transmisión cifrada on-line desde el centro de gestión.

Generación y distribución de claves:
-Generadas por el propio equipo a partir de la semilla introducida manualmente.
-Generadas en el Centro de Gestión del punto 2.4 para cargar en una tarjeta electrónica o transmisión cifrada.

Características operativas:
Como cifrador de datos:
-En líneas RTB se comportará como un modem-cifrador controlable mediante parámetros AT, según normas ITU-T hasta 31.2 Kbps. En esta modalidad, será inter operable con los cifradores de datos anteriormente suministrados por EPICOM a la Armada.
-En líneas RDSI y mediante un adaptador o moden externo a 64/128 Kbps.

## Cifrador IP EP-430C.

Cifrador para servicios de seguridad a las comunicaciones basadas en el protocolo TCP-IP.

Características generales:

- Nivel Físico: 10BaseT con posibilidad de instalar AUI.
- Nivel de enlace: Ethernet/IEEE 802.3.
- Recomposición de los datagramas fraccionados en su tránsito por la red.
- Operación transparente a todos los protocolos entre zonas rojas.
- Tráfico cifrado y encapsulado en datagramas UDP.
- CONFIDENCIALIDAD: Cifrado por suma módulo 2 con la serie cifrante. Algoritmo simétrico.
- IDENTIDAD USUARIOS: Cifrado de los datagarmas IP incluyendo la cabecera.
- INTEGRIDAD de los datos, utilizando mecanismos asociados al cifrado.
- AUENTICACION de origen y destino, utilizando propiedades del Sistema de Gestión de claves EPICOM.
- CONTROL DE ACCESO, mediante tarjeta electrónica grabada en el Centro de Gestión.
- Protecciones contra "replay" y otros ataques.

Protecciones:

-Borrado automático de claves en caso de apertura de la caja o mediante pulsador en panel frontal.
- Auditorías. Registro automático de alarmas y eventos significativos.
- Autenticación del software.
- Identidad del cifrador basada en un número de serie interno inviolable.
- Supervivencia de la red en caso de captura de las claves de un cifrador. Información de claves almacenada en cada cifrador debe ser UNICA en la red.
- Diseño TEMPEST.

Gestión de claves:

- Capacidad para 10 bancos de Claves, que permiten formar grupos cerrados de usuarios.
- Claves únicas e irrepetibles para cada datagrama IP.
- Claves de Asociación de Seguridad exclusivas para cada posible pareja de cifradores y diferentes cada vez que se establece la Asociación entre dos cifradores.

Carga de Claves:

-Manual, a través del teclado del teléfono asociado.
-Por medio de tarjeta electrónica
-Por transmisión cifrada on-line desde el centro de gestión.

Generación y distribución de claves:

-Generadas por el propio equipo a partir de la semilla introducida manualmente.
-Generadas en el Centro de Gestión del punto 2.4 para cargar en una tarjeta electrónica o transmisión cifrada.

Características operativas:

Como cifrador de datos:
-En líneas RTB se comportará como un modem-cifrador controlable mediante parámetros AT, según normas ITU-T hasta 10 Mbps. En esta modalidad, será inter operable con los cifradores de datos anteriormente suministrados por EPICOM a la Armada.
-En líneas RDSI y mediante un adaptador o moden externo a 10 Mbps.

**3.- PRUEBAS DE RECEPCION.**

Los sistemas se recepcionarán en el Gabinete Cripto de la Armada una vez

efectuadas pruebas de que demuestren las funcionalidades exigidas.

## 4.- APOYO LOGISTICO.

El Contratista presentará una Propuesta de Apoyo Logístico, que al menos debe comprender:

4.1. Documentación técnica.

Se suministrará un manual descriptivo de los equipos en español.

4.2. Configuración.

El contratista deberá entregar el diagrama de bloques del Sistema, que sirva para que la Armada pueda elaborar la documentación de configuración correspondiente.

## 4. ASEGURAMIENTO DE LA CALIDAD

5.1. El presente contrato está sujeto a la inspección oficial de aseguramiento de la calidad, designada por la Dirección general de Armamento y Material.

5.2 El sistema de calidad aplicable es el establecido por la Publicación Española de Calidad PECAL 2120.

## 6. CATALOGACIÓN

De conformidad con el STANAG 4177, ratificado por España y conforme con el Real Decreto 166/2010, el contratista deberá, caso de no haberlo hecho con anterioridad catalogar los artículos objetos de este suministro de acuerdo con lo dispuesto en esta cláusula y el Real Decreto referido.

a) El contratista está obligado a proporcionar, al escalón de catalogación que se designe (SUBDEM) y en el plazo que se establezca (en los pedidos de material quincenales, indicados en el Pto. 4 de este PPT), primeramente una lista con la identidad del fabricante verdadero y el número de pieza y nombre o designación con que dicho fabricante identifica cada artículo objeto del contrato y, en su caso, de los repuestos acordados como necesarios para asegurar el servicio de mantenimiento de los mismos por la organización logística usuaria y, además, cuantos documentos de carácter técnico suficiente se le requieran por ser necesarios para establecer y controlar los datos de identificación de los artículos.

b) El contratista está obligado a proporcionar igualmente, al escalón de catalogación designado como competente y en el plazo que se establezca, la documentación

técnica definitoria de las características físicas y funcionales de aquellos artículos de la lista anterior que resulten no estar catalogados y/o las propuestas de identificación de los mismo, de conformidad con el Sistema OTAN de Codificación y las normas e instrucciones del citado escalón competente y, adicionalmente, las especificadas en este pliego de prescripciones técnicas.

c) El contratista será responsable único respecto a la obtención de sus subcontratistas o proveedores, de los datos técnicos necesarios para la identificación de los artículos a catalogar, así como de la presentación en plazo de estos datos y/o de las propuestas de catalogación correspondientes ante el escalón competente.

d) El contratista está obligado a proporcionar los datos de actualización relativos a todas las modificaciones de identificación o fabricación incorporadas a los materiales o piezas de repuesto relacionados en la lista indicada en el párrafo a) anterior, que puedan acontecer durante la ejecución y garantía del contrato, así como cuantos otros datos complementarios o de gestión sean de interés para la organización logística usuaria.

e) El contratista está obligado a justificar el cumplimiento de la catalogación estipulada en esta cláusula, mediante certificado que deberá recabar del escalón de catalogación designado como competente para el contrato y que será necesario para la liquidación del mismo; entendiéndose no finalizada la entrega de los bienes objeto del contrato en tanto no sean cumplimentadas plenamente las obligaciones de catalogación estipuladas, a las que, expresamente, se conferirá el carácter de obligaciones principales e inherentes a la propia entrega de los artículos, de modo que su incumplimiento deberá tener el mismo tratamiento y efectos que el incumplimiento de la obligación de la entrega.

Para cualquier aclaración referente a esta Cláusula, el contratista deberá solicitar información en la Sección de Material y Cargos de la DAT (Dirección de Aprovisionamiento y Transporte) de la JAL (Jefatura de Apoyo Logístico de la Armada. Avda. de Pío XII núm. 83. 28036 Madrid.

## 7. CLAUSULA DE IGUALDAD DE OPORTUNIDADES.

Dada la naturaleza de este contrato, no es posible definir estas prescripciones técnicas en condiciones de igualdad que permitan la concurrencia de cualquier licitador, tal y como establece el art. 19 del LCSPDS 24/2011.

## 8. COMPATIBILIDAD CON LOS PROTOCOLOS DE IPv6

Todo sistema (hardware, software, firmware, etc) o servicio relacionado directa o indirectamente con la transmisión, manipulación o procesamiento de información por medio del protocolo IP, independientemente del régimen bajo el cual se regule la

relación con dicho elemento (adquisición, desarrollo, explotación, contratación, etc.), debe ser capaz de operar plenamente de acuerdo a los estándares comerciales establecidos para el protocolo "IPv6" y a los aspectos definidos en el RFC 2460 (Internet Protocol Versión 6 Specification) y el resto deRFC relacionados con "IPv6".

En esta circunstancia, el sistema o servicio debe mantener o mejorar los niveles de servicio, calidad y confianza preestablecidos, tanto con el protocolo "IPv4" como con "IPv6", asimismo, la empresa adjudicataria del contrato deberá aportar, durante el periodo de garantía establecido o el que se marque en este Pliego, soporte técnico para ambos protocolos.

Madrid, 7 de Mayo de 2014.




Fuente : www.armada.mde.es/contratos/doc/3-50-40-14-483-PPT.PDF