

Trabajo Fin de Grado

DESARROLLO DE LAS COMUNICACIONES DE VOZ IP A TRAVÉS DEL CALL MANAGER

Alberto Pablo González García

Director académico: Domenico Sicignano

Director militar: Miguel García Montero

Centro Universitario de la Defensa-Academia General Militar

2022



Agradecimientos

En primer lugar, me gustaría agradecer a mi familia, desde padres y hermana en Madrid, hasta tíos y primos aquí en Zaragoza, que me han cuidado y aguantado mientras hacia este TFG. Me han acogido en sus casas y yo les he estado transmitiendo mis inquietudes diarias a la hora de su realización. Han tenido mucha paciencia y calidad humana, gracias.

Seguidamente quiero agradecer a la unidad de élite que es la BRIPAC, por haberme acogido en su seno de una manera tan cercana. Desde el General Jefe de la BRIPAC Excelentísimo Señor, Don Luis Jesús Fernández Herrero por dejarnos realizar las prácticas en ella, pasando por el Teniente Coronel Don Joaquín Sanjuan Garcia Jefe del Batallón de Cuartel General, que tan bien nos recibió y nos trató.

Especial agradecimiento a la Compañía de Transmisiones, desde el capitán, hasta el último soldado. El Capitán Jede de la CIA, y mi tutor militar, Don Miguel Garcia Montero, que aún están muy ocupado, puedo atender mis dudas y darme consejos para realizar este trabajo, sin olvidar sus charlas motivadoras para seguir adelante que no olvidare. Los Tenientes Jefes de Sección, en especial y Don Carlos de Diego Lara, este aparte mi segundo tutor militar, Don José Antonio Ortiz Sánchez, que tan bien me guiaron y acompañaron durante las practicas. A los Sargento Primero Don Álvaro Gómez Gonzalo y Don Santiago Vicente Santander Rosero que, con su dilatada experiencia y conocimiento, me aportaron la información técnica necesaria para la elaboración del proyecto. Los Sargento Víctor Morcillo Scholl y Rafael Álvarez Castaño que me guiaron y enseñaron a realizar los ejercicios prácticos de operador de CM. Los que me enseñaron sus posibilidades, sus capacidades y alcance de desarrollo. Sus juicios y valoraciones están sintetizadas en este trabajo. Sin duda todos ellos grandes profesionales a los que confiaría sin dudar cualquier aspecto laboral o de cualquier índole. Alguno de ellos viejos amigos y otros nuevos. Y, por último, la sangre del Ejercito y la compañía, La Tropa. El caballo de batalla que hace a los mandos entre otras cosas, la vida más fácil a la hora de dirigir y operar los equipos. Me ayudaron y enseñaron el montaje de los equipos a utilizar, algunos incluso saben operar pues la formación que reciben en la Compañía obliga al desempeño de esta función.

Especial atención a mi tutor civil Don Domenico Sicignano. Sus aportaciones a este trabajo en modo de consejo y corrección son inestimables, más cuando debido a haber sido padre, ha atendido mi trabajo haciendo un esfuerzo doble. Sobre todo, porque el tiempo apremiaba, y eso se valora mucho.





RESUMEN

El objetivo este trabajo fin de grado es el de analizar las centralitas telefónicas de trabajo de Voz sobre IP (VoIP) en dotación en el Ejército para conocer su funcionamiento y discernir cuál de las centrales se ajusta en mayor medida a las necesidades actuales de la Brigada Paracaidista y por extensión del Ejército de Tierra. Para este fin, se tendrán 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 del sistema en una red. Teniendo en cuenta siempre la integración del equipo con el resto de los medios del arma de Transmisiones.

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 de este. La importancia crítica de la Voz sobre IP para el futuro del Ejército, la urgente necesidad de modernización de los sistemas de comunicación telefónica, su unificación 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 y su explotación de la manera más eficaz.

El resultado final del Trabajo es, que una persona con conocimientos iniciales se haga una idea de la situación de nuestro Ejército de Tierra con respecto al desarrollo de la VoIP y pueda entender la importancia de las transmisiones en general y el equipo en estudio en particular.

Palabras clave

Voz sobre IP

Central telefónica

Comunicaciones

Ancho de Banda



ABSTRACT

The goal of this final degree project is to analyze the telephone switchboards based on the Voice over IP (VoIP) used in the Army to know how they work. Then, the objective is to discern which of the stations best suits the current needs of the Parachute Brigade and by extension of the Army, considering the characteristics and specifications that a communications equipment must have for its use in the Armed Forces.

For this, the fundamentals of VoIP are studied in a general way to later make a study of the stations in the Army. In the analysis carried out on the exchanges, the key aspects of VoIP in the Army are studied, such as bandwidth, security, management, services, and the necessary budget for the implementation of the system in a network. Always considering the integration of the equipment with the rest of the means of the Transmissions weapon.

Finally, the Final Degree Project is concluded with a critical judgment on the tests and exercises carried out. In the last part of the work the conclusions drawn during the realization of this are exposed. The critical importance of Voice over IP for the future of the Army, the urgent need to modernize telephone communication systems, their unification and the conclusions drawn from each of the field tests carried out, as well as the proposal for future lines of work to make VoIP a reality in the Army and its exploitation in the most effective way.

The result of the Work is that a person with initial knowledge gets an idea of the situation of our Army with respect to the development of VoIP and can understand the importance of transmissions in general and the equipment under study.

KEYWORDS

Voice over IP

CallManager

Communications

Bandwidth



INDICE DE CONTENIDO

Contenido

Agradecimientos	I
RESUMEN	II
Palabras clave	II
ABSTRACT.....	III
KEYWORDS	III
INDICE DE FIGURAS	VI
INDICE DE TABLAS.....	VII
ABREVIATURAS, SIGLAS Y ACRÓNIMOS.....	VIII
1 INTRODUCCIÓN.....	1
2 OBJETIVOS Y METODOLOGÍA.....	2
2.1 OBJETIVOS Y ALCANCE	2
2.2 METODOLOGÍA	2
2.3 ESTRUCTURA DE LA MEMORIA	3
3 ANTECEDENTES Y MARCO TEÓRICO.....	4
3.1 FUNDAMENTOS DE LA TELEFONÍA IP	4
3.2 INTRODUCCIÓN A LA VOZ SOBRE IP (VoIP)	5
3.3 HISTORIA DE LA VoIP	5
3.4 ESTADO ACTUAL Y EVOLUCIÓN DE LA VoIP.....	6
3.5 VENTAJAS DE LA VoIP	8
4 DESCRIPCIÓN ASPECTOS TECNOLÓGICOS.....	10
4.1 PROTOCOLOS DE SEÑALIZACIÓN	10



4.2	SEÑALIZACIÓN EN REDES TELEFÓNICAS ANALÓGICAS	11
4.3	H.323	12
4.4	SIP (Session Initiation Protocol)	13
4.4.1	Arquitectura de SIP	13
4.4.2	Formato de los mensajes SIP	14
4.4.3	Intercambio de mensajes SIP	15
4.4.4	SCCP (Skinny Call Control Protocol)	17
4.4.5	MGCP (Media Control Protocol)	17
4.4.6	Protocolo IAX2	18
4.5	CODECS Y FACTORES A TENER EN CUENTA EN VoIP.	18
4.5.1	Factores críticos en VoIP	19
4.5.2	Mecanismos de corrección	21
4.5.3	CÓDECS	21
4.6	MATRIZ DE RIESGOS	37
5	DESARROLLO: ANÁLISIS Y RESULTADOS.....	24
5.1	MEDIOS EN DOTACION EN LA UNIDAD Y EJERCICIO PRACTICO	25
5.1.1	Requerimientos técnicos de las centrales de VoIP	26
5.2	GESTIÓN DE LAS CENTRALES	29
5.2.1	Servicios y compatibilidades	33
5.2.2	Presupuestos.....	34
5.3	CUADRO DAFO.....	40
6	COMPARACIÓN DE LOS SISTEMAS DE VoIP	41
6.1	ANCHO DE BANDA	41
6.2	SEGURIDAD	42
6.3	GESTIÓN	42



6.4	SERVICIOS Y COMPATIBILIDADES.....	43
6.5	PRESUPUESTO	43
6.6	ELECCIÓN DE CENTRAL.....	43
7	CONCLUSIONES	43
7.1	LINEAS FUTURAS.....	44
8	REFERENCIAS BIBLIOGRÁFICAS	45

INDICE DE FIGURAS

Figura 1. Flujo de codificación/decodificación. Fuente: JK Sistemas y comunicaciones	4
Figura 2. Puertos FXS/FXO. Fuente: JK Sistemas y comunicaciones	5
Figura 3. FXO Gateway. Fuente: JK sistemas y comunicaciones	5
Figura 4. Número de abonados y proporción de líneas principales. Fuente:iDATE	7
Figura 5. Comunicaciones Unificadas. Fuente: 3CX	8
Figura 6. Costes. Fuente: Sarenet	9
Figura 7. SS7 arquitectura. Fuente: Univ. Cauca	11
Figura 8. Uso del protocolo H.323 entre terminales. Fuente: 3CX	12
Figura 9. Ejemplo de arquitectura basada en H.323. Fuente: Server VoIP	13
Figura 10. SIP Protocolos usados. Fuente: Vozonline.	14
Figura 11. Flujo de llamada SIP entre extensiones IP-PBX. Fuente: 3CU electrónica	16
Figura 12. Posibles causas de latencia. Fuente: Gesditel	19
Figura 13: Códecs VoIP. Fuente: Sip Systems.....	22
Figura 14. Muestreo. Fuente: Systemvan	23



Figura 15. Cuantificación. Fuente: Wikiwand	23
Figura 16. Codificación. Fuente: ikastaroak	24
Figura 17. Cisco CM 2811. Fuente: Propia	25
Figura 18. Esquema orientativo maniobra. Fuente: Propia	26
Figura 19. CM estándar. Fuente: Configuración CME ppt.	26
Figura 20 Esquema de un Centro de Transmisiones.....	29
Figura 21. Organigrama BRIPAC. Fuente: Propia	30
Figura 22. Línea de comandos en CM Cisco. Fuente: Propia	32
Figura 23. Configuración CM Asterisk Tripbox. Fuente: Propia.....	32
Figura 24. Consumos códecs. Fuente: VoIP	34
Figura 25. Tarjetas FXO, FXS para Cisco. Fuente Cisco	36
Figura 26. Consumo llamada VoIP. Fuente: OpManager	42
Figura 27. Extracto de organización. Fuente: Defensa.....	81

INDICE DE TABLAS

Tabla 1. Tipos de Cifradores. Fuente: MinisDef.....	29
Tabla 2. Precios para sistema Asterisk. Fuente: Propia	35
Tabla 3. Precios para sistema Cisco. Fuente: Propia	36
Tabla 4. Presupuesto total sistema Asterisk. Fuente: Propia	37
Tabla 5. Presupuesto total sistema Cisco. Fuente: Propia	37
Tabla 6. Matriz de Riesgos. Fuente: Propia	39
Tabla 7. Tabla de cantidad de nivel de riesgos de la Matriz de riesgos. Fuente: Propia	40
Tabla 8. Análisis DAFO. Fuente: Propia	41



ABREVIATURAS, SIGLAS Y ACRÓNIMOS

BRI: Basic Rate Interface o Interfaz de Servicio básico. Call leg: es un segmento discreto de una conexión de una llamada, la cual se encuentra entre dos puntos de la conexión. Por ejemplo, entre el teléfono y el Router, entre el Router y la red, entre el Router y un PBX.

CGES: Centro Gestor de Elementos Secretos. Departamento donde se gestionan las claves secretas del Ejército.

CIS: Sistemas de Información y Telecomunicaciones / Communication and Information Systems.

CM: Call Manager, Una centralita VoIP, o también llamada centralita IP, es un sistema de telefonía para empresas donde la señal se transmite por internet. La palabra VoIP viene del inglés, Voice Over IP, y se traduce como voz sobre IP, y funciona usando los distintos protocolos de voz por IP.

FXO: FXO (Foreign Exchange Office, en inglés) es un dispositivo de computador que permite conectar éste a la RTC, y mediante un software especial, realizar y recibir llamadas de teléfono. Sirve sobre todo para implementar centralitas telefónicas (PBX) con un ordenador.

FXS: FXS (Foreign Exchange Station) es el conector en una central telefónica o en la pared de nuestro hogar, que permite conectar un teléfono analógico normal.

IP: Internet Protocol - Protocolo de Internet. Este protocolo es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de vídeo o la conexión a un sitio web. Una dirección IP identifica una red o dispositivo en Internet.

IPS o Shoftphone: Un softphone (en inglés combinación de software y de telephone) es un software que es utilizado para realizar llamadas a otros softphones o a otros teléfonos convencionales usando un VoIP (Voz sobre IP) o ToIP (Telefonía sobre IP) desde un ordenador, por ejemplo.

ISDN: Integrated Services Digital Network - Red digital de servicios integrados. Establece los estándares para la transmisión de voz, vídeo, datos y otras señales digitales mediante el servicio de telefonía por hilo de cobre que usa la Red de telefonía pública conmutada (RTC).

ITU: La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. Su sede se encuentra en la ciudad de Ginebra (Suiza).

NAT: El término NAT es la abreviatura de Network Address Translation o direcciones de red. Es el proceso mediante el cual una o más direcciones locales (local address) se traducen en una o más direcciones globales (global IP address) y viceversa, con el fin de proporcionar acceso a internet a los hosts locales.

PBX: Un PBX o PABX (siglas en inglés de Private Branch Exchange) Central Privada Automática; es en realidad cualquier central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica.



PCM: La modulación por impulsos codificados (PCM por sus siglas inglesas de Pulse Code Modulation) es un procedimiento de modulación utilizado para transformar una señal analógica en una secuencia de bits.

PSTN: La PSTN es La Red Telefónica Pública Conmutada, las llamadas locales y de larga distancia son posibles gracias a ella. Se trata de una red telefónica clásica en donde se da una comunicación de voz en tiempo real, asegurando fluidez en el tráfico de la red.

QoS: La calidad de servicio (quality of service o QoS) se refiere a cualquier tecnología que gestiona el tráfico de datos para reducir la pérdida de paquetes, la latencia y el jitter, o fluctuación, en una red.

RBA: Red Básica de Área, La Red Básica de Área (RBA), es la principal red de telecomunicaciones militar a través de la cual se integran diversos medios CIS para poder proporcionar servicios a los usuarios militares. Actualmente obsoleta.

RFC: Los Request for Comments, más conocidos por sus siglas RFC, son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos. Se van numerando por ejemplo el 3261.

RTC: La red telefónica conmutada (RTC) se define como el conjunto de elementos constituido por todos los medios de transmisión y conmutación necesarios para enlazar a voluntad dos equipos terminales mediante un circuito físico, específico para la comunicación. Se trata, por tanto, de una red de telecomunicaciones conmutada.

TCP: Protocolo de control de transmisión (en inglés Transmission Control Protocol o TCP) es uno de los protocolos fundamentales en Internet. Está ubicado en la capa de transporte del modelo OSI. El objetivo del protocolo TCP es crear conexiones dentro de una red de datos compuesta por redes de computadoras para intercambiar datos.

UDP: El protocolo de datagramas de usuario (en inglés: User Datagram Protocol o UDP) es un protocolo del nivel de transporte basado en la transmisión sin conexión de datagramas y representa una alternativa al protocolo TCP (Transmisión Control Protocol).

UTP: UTP (Unshielded Twisted Pair – Par trenzado no apantallado): Es un cable sin apantallamiento. Esto lo sigue haciendo bueno para utilizar en casa, por ejemplo, para conectar tu ordenador, NAS o cualquier otro dispositivo al router



1 INTRODUCCIÓN

En nuestras fuerzas armadas hay una especialidad fundamental, o arma, denominada Transmisiones. Esta especialidad, encargada del enlace entre los puestos de mando y sus unidades subordinadas, se encuentra inmerso en una constante actualización y modernización tanto de equipos como de doctrina. Y esto es así porque nos basamos mucho en las telecomunicaciones y toda la tecnología de software y hardware en la que se asienta.

El ejército en lo relacionado a la comunicación por voz usaba los medios radio para cumplir la misión casi exclusivamente. Aun las sigue usando. Esto significa que la comunicación es dúplex, en ambos sentidos, pero no full dúplex. Esto quiere decir, primero hablaba uno y acto seguido el otro, sin la posibilidad de hablar los dos al mismo tiempo, teniendo que usar un lenguaje convenido y un procedimiento radio, dando a veces problemas en la comunicación de mal entendidos o lentitud en las órdenes si las circunstancias son adversas.

A parte de los medios radio, se utiliza la infraestructura de los cuarteles para el uso de la telefonía, por no hablar de un antiguo sistema llamado RBA (Red Básica de Área). Todos estos medios usaban telefonía analógica o a dos hilos. Si bien la RBA ha desaparecido, el sistema de dos hilos ISDN (Integrated Services Digital Network - Red Digital de Servicios Integrados), de los cuarteles está en proceso de modernización gracias también a los CM (Call Manager), usando la red de datos, cambiando los dos hilos e implementando la red de cable UTP (Unshielded Twisted Pair – Par trenzado no apantallado).

Esto se solucionó parcialmente con la telefonía con medios satélite. El problema es que los terminales con gran capacidad son pesados y complejos. Por no hablar que la centralita de un terminal satélite IP (Internet Protocol - Protocolo de Internet) está preparada de tal forma que solo CGES (Centro de Gestión de Espectro) pueda configurarla, por lo que es imposible su configuración a nivel operador.

El ejército en su constante modernización decidió que a través de la red (infraestructura) de datos IP, pasar la voz, ósea VoIP, ya sea en instalaciones como en el campo, que es lo que nos preocupa a nosotros. Para realizar esto, se necesita un router IP con un software de digitalización de voz o Call Manager que después de una configuración, permite ir conectando teléfonos y permitir llamadas entre ellos, pudiendo interconectar más medios y escalar la red para que las llamadas lleguen más y más lejos. Se puede configurar ese router a placer, desde poner solo dos usuarios a poder poner cientos y miles, haciendo pasar el servicio por diferentes medios de transmisión y soportes. Permitiendo una redundancia y, por ende, un extra de seguridad que el Ejército valora sobremanera. Esto permite que si por las circunstancias del medio ambiente, la orografía o la misión cayese un soporte, el enrutamiento dinámico del CM junto con el resto de los equipos intermedios, redirigiría las comunicaciones de tal forma que el servicio de voz seguiría funcionando. Incluso esta redundancia se puede triplicar, permitiendo que la acción del mando por voz se mantenga arriba incluso en las circunstancias más adversas gracias a este equipo, el Call Manager y el soporte del resto de medios.

Este trabajo tiene como finalidad, encontrar un Call Manager que se ajuste a las necesidades de esta unidad en la que realizo las practicas, ósea, la Brigada Almogávares VI, Brigada Paracaidista del Ejército de Tierra, pero que se pueda implementar esta solución para cualquier brigada del Ejército de Tierra, ya sea ligera, o mecanizada. A parte, se ha estudiado las capacidades de los Call Manager presentes en la unidad realizando una práctica real.



2 OBJETIVOS Y METODOLOGÍA

2.1 OBJETIVOS Y ALCANCE

El objetivo para este Trabajo de Fin de Grado es saber qué posibilidades tienen los call Manager en cuanto a sus capacidades y utilidad para la Brigada Paracaidista y por extensión, cualquier brigada del ET y así deducir que modelo es el más apropiado.

Antes de escribir el trabajo, tuvieron lugar unos ejercicios de Instrucción y Adiestramiento especializados en el conocimiento CIS (Sistemas de Información y Telecomunicaciones / Communication and Information Systems.) con la Compañía de Transmisiones de la BRIPAC para usar y conocer mediante la práctica qué es y qué utilidad tiene un Call Manager para así conocer el desempeño del equipo. Esto permitió tener unas bases aceptables de conocimiento para poder analizar qué equipo sería el ideal para esta unidad, comparando en el futuro que productos ofrece el mercado de los Call Manager y explicar, con una conclusión, el motivo de la elección.

En cuanto a los medios disponibles de VoIP, la Compañía de Transmisiones del Batallón de Cuartel General de la BRIPAC dispone de dos centrales casi idénticas, las centrales proporcionadas por la empresa Cisco llamadas Call Manager, con softwares casi idénticos, llamadas Águila, la principal y Buitre la secundaria y por otro lado la central desarrollada por la empresa Digium llamada Asterisk, en su versión virtualizada para ser instalada en un ordenador.

A nivel Brigada y Ejército se debe encontrar una solución a esta dualidad debido al gasto ineficiente de presupuesto y dificultad que plantea el tener dos medios 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 esta.

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, profundizar en el conocimiento de esta tecnología, así como explicar el proceso de diseño e implementación de una infraestructura en un caso real. Además, se redactarán las características que debe cumplir una central de VoIP para su servicio en la Brigada y por extensión en el Ejército de Tierra.

Se usará la misma red utilizada en maniobras, añadiendo más equipos CM o medios de transmisión, así como usando el simulador de Packet Tracer previamente para mostrar de manera limpia como trabajaría esta red simulada antes de montar realmente la práctica y ver hasta cuanto podemos ajustar la teoría a la realidad. Pudiendo así exprimir al máximo el equipo.

2.2 METODOLOGÍA

Para llevar a cabo este Trabajo de Fin de Grado, se ha utilizado la siguiente metodología en las practicas externas en la Compañía de Transmisiones del Batallón de Cuartel General de la Brigada Paracaidista Almogávares VI del Ejército de Tierra de Paracuellos del Jarama.

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 una fase de pruebas de campo y maniobras las cuales han ocupado dos semanas de las prácticas, una de preparación, y otra de trabajo de campo propiamente dicho. 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. La observación y la revisión documental fueron claves en este periodo del trabajo. Acto seguido se centró el estudio en torno al resultado de dichas pruebas. Para ello se realizaron unas prácticas con la debida configuración de cada una de las centrales con sus respectivos medios para asentar los conocimientos adquiridos en las pruebas de la semana de campo y sintetizar dichas pruebas solo al estudio del CM. Hasta este punto, los métodos usados fueron, la investigación de las centrales y sus posibilidades, así como unas encuestas a los mandos responsables de los equipos. Posteriormente se realizó un análisis de la información recopilada para comprender las dificultades debidas a la dualidad de sistemas y el funcionamiento de estas, así como sus ventajas y vulnerabilidades de cada centralita.

Finalmente se estudió la puesta en marcha de cada una de ellas 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.

2.3 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 tema. Por ello la primera parte de esta memoria es la introducción, en la cual se la situación actual de las transmisiones y de la VoIP en general a nivel civil. La importancia que tienen las transmisiones para el Ejército y sus ventajas. En segundo lugar, se exponen los aspectos tecnológicos que involucran a este sistema de telefonía. Protocolos de señalización, códecs y arquitectura básica para entender la parte interna y los tecnicismos de la VoIP y del equipo a analizar. A parte se analizan los riesgos con una matriz que permite situar al lector en el contexto técnico con respecto a los desafíos actuales. El tercer punto es el desarrollo y análisis de resultados de las centrales a estudio. Incluyendo los presupuestos para cada equipo. Por último, se hace una comparación y justificación de los resultados obtenidos en el Trabajo, finalizando con una conclusión.



3 ANTECEDENTES Y MARCO TEÓRICO

En este capítulo, se tratarán aspectos técnicos básicos para poder introducir al lector en el mundo sobre el protocolo IP. Y asegurarse un entendimiento posterior al análisis de las centralitas telefónicas sobre IP.

3.1 FUNDAMENTOS DE LA TELEFONÍA IP

Hace unos años en los cuarteles existían dos infraestructuras independientes de red. Una para datos, red IP, y otra para voz, la cual era analógica. De hecho, aún es así en algunos cuarteles.

El perfeccionamiento de las redes IP, el desarrollo de las técnicas para la digitalización de la voz, así como mecanismos de control de flujo y priorización de tráfico, originó la posibilidad de la transmisión de voz a través de la red de datos con una calidad competente. A esta tecnología se le conoce como VoIP (*Voice over Internet Protocol*).

Debido a lo expuesto anteriormente, se consiguió cambiar el concepto de comunicación desde la conmutación de circuitos a la comunicación de conmutación de paquetes.

El concepto original se basa en transformar la voz en paquetes de información adecuados para una red tipo IP que, ayudada por otros protocolos de conmutación y la reserva de un ancho de banda adecuado, se pueda garantizar una buena comunicación.

Para transformar la voz en paquetes se usa un proceso llamado digitalización. Este proceso consiste en transformar la voz (es una señal analógica) en señales PCM (*Pulse Code Modulation*) por medio del codificador de voz (códec). Estas muestras PCM pasan por un algoritmo de compresión, el cual comprime la voz y la fracciona en paquetes IP. Tras esto son enviados a través de la red IP a su destinatario.

En la figura 1 se puede ver un ejemplo de una conversación extremo a extremo de una comunicación utilizando VoIP.

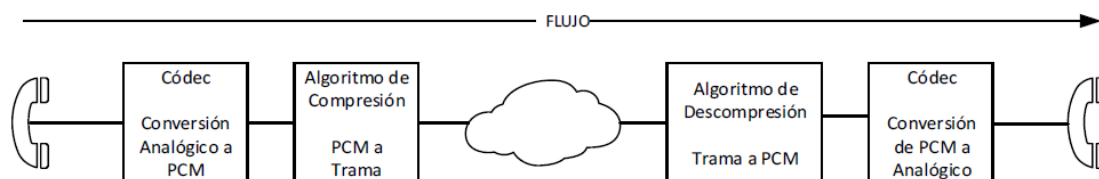


Figura 1. Flujo de codificación/decodificación. Fuente: JK Sistemas y comunicaciones

La interconexión entre el mundo analógico y el mundo IP se realiza entre dispositivos denominados gateways si nos referimos a la telefonía. Estos equipos realizan la codificación y direccionamiento del paquete IP para que se transmita a la PSTN (Public Switched Telephone Network) y viceversa.



3.2 INTRODUCCIÓN A LA VOZ SOBRE IP (VoIP)

Para interconectar las diferentes redes de datos IP con la PSTN, se necesita de los dispositivos gateways mencionados anteriormente, pudiéndose usar como codificadores. Estos equipos poseen dos tipos de tarjetas dependiendo de la dirección de conversión. FXS (Foreing Exchange Station) para teléfonos dentro de las redes IP y FXO (Foreing Exchange Office) si el teléfono está conectado a la PSTN.



Figura 2. Puertos FXS/FXO. Fuente: JK Sistemas y comunicaciones

En la figura 2 se puede ver como sería la interconexión con una centralita analógica, en donde los puertos FXO conectarían con los FXS y estos a los teléfonos analógicos. En la figura 3 vemos como con una tarjeta FXO podríamos interconectar una empresa de telefonía y nuestra propia centralita IP.

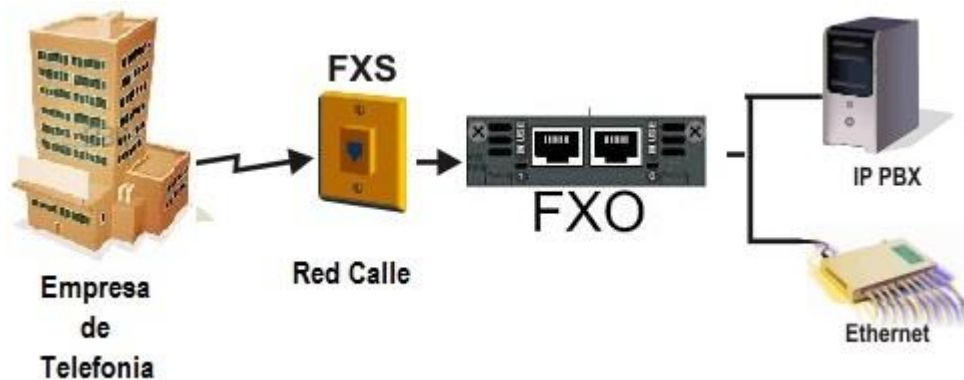


Figura 3. FXO Gateway. Fuente: JK sistemas y comunicaciones

En el caso de las comunicaciones militares, el transporte a dos hilos es digital, pero las estaciones ya tienen diferentes equipos de digitalización para reconvertir la señal a una señal IP.

3.3 HISTORIA DE LA VoIP

La historia de la VoIP es relativamente reciente comparada con las transmisiones



eléctricas en general. Comenzó debido a los trabajos realizados por unos israelitas allá por 1995. La comunicación era de ordenador a ordenador. Vocaltec, una empresa hebrea de telecomunicaciones lanzo al mercado el primer IPS llamado "Internet Phone Software".

En 1997, Jeff Pulver consiguió juntar a usuarios, fabricantes y persinas interesadas en esta tecnología creando el mayor evento anual de VoIP.

En 1998, un grupo de emprendedores comenzó a fabricar los primeros adaptadores de teléfonos analógicos y Gateways que permitían la comunicación desde un ordenador hasta un teléfono convencional (PSTN) y entre teléfonos convencionales usando convertidores de extremo a extremo.

En 1999 la empresa de equipos de telecomunicaciones e informáticos vende las primeras plataformas corporativas de VoIP usando para ello el protocolo de señalización H.323, convirtiéndose así en la primera empresa en dar estas soluciones.

En el 2000, un estudiante llamado Mark Spencer de la universidad de Auburn en Alabama, crea Asterisk, la primera central telefónica basada en Linux con un código de fuente abierto.

En 2002 surge el protocolo de señalización SIP y este comienza a sustituir al H323. Ya en 2003, los universitarios Jan Friis y Niklas Zenntrom, crearon un softphone gratuito que podía instalarse fácilmente en cualquier PC pudiendo así atravesar todos los firewalls, así como funcionar en cualquier router, inclusive los corporativos tal como Skype. Skype se caracteriza por rodar con un protocolo propietario que permite la compresión para mejorar la calidad de voz.

En los últimos años y ya hasta la actualidad, la VoIP se está imponiendo como tecnología de comunicaciones debido a los avances en los equipos que soportan ésta [\[1\]](#).

3.4 ESTADO ACTUAL Y EVOLUCIÓN DE LA VoIP

Actualmente el volumen del tráfico de VoIP es variable. Pero si se sabe que tanto las empresas como organismos gubernamentales están migrando a este sistema por su sencillez y calidad. Así que se puede asegurar que el tráfico aumenta como podemos ver en el gráfico de la figura 4.

Según la web Unión Internacional de Telecomunicaciones la VoIP aumenta de manera clara.

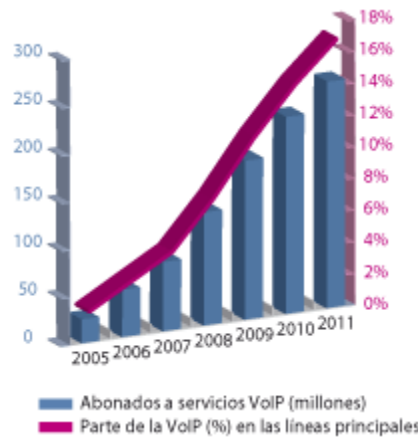


Figura 4. Número de abonados y proporción de líneas principales. Fuente:iDATE

El volumen de negocio VoIP se estima en más de 100.000 millones de dólares a nivel mundial para 2026, y la cifra no para de crecer. Todos los negocios relacionados con la VoIP como las PBX, o los servicios asociados tienen grandes beneficios, y unos crecimientos anuales prometedores. En algunos países hay un "mercado gris" de servicios VoIP que no son realmente legales, y los operadores legítimos anuncian pérdidas de ingresos sustanciales. En Pakistán, por ejemplo, el regulador de las telecomunicaciones dice que el tráfico gris le cuesta 50 millones USD al año. El mercado gris en los países africanos también es considerable. El operador nigeriano Nitel, por ejemplo, estimó que antes de que en 2004 redujera el precio de las llamadas internacionales, 90% de esas llamadas se efectuaban a través del mercado gris [2] [3].

A parte la tendencia de esta tecnología es la de dar los servicios a las empresas y organismos a través de un servicio en la nube que permite tener los equipos en las empresas almacenados y seguros y aun así dar servicios personalizados a cada cliente de manera barata.

Por no hablar de los servicios de Comunicaciones Unificadas. Que consiste en tener varios servicios como la telefonía, la mensajería unificada (correo electrónico, buzón de voz y fax), mensajería instantánea corporativa, conferencias web y videollamadas, todo en un solo soporte ya sea físico o virtual. En la figura 5 se aprecia como la VoIP es utilizada en todos los servicios actuales con las comunicaciones unificadas [4].

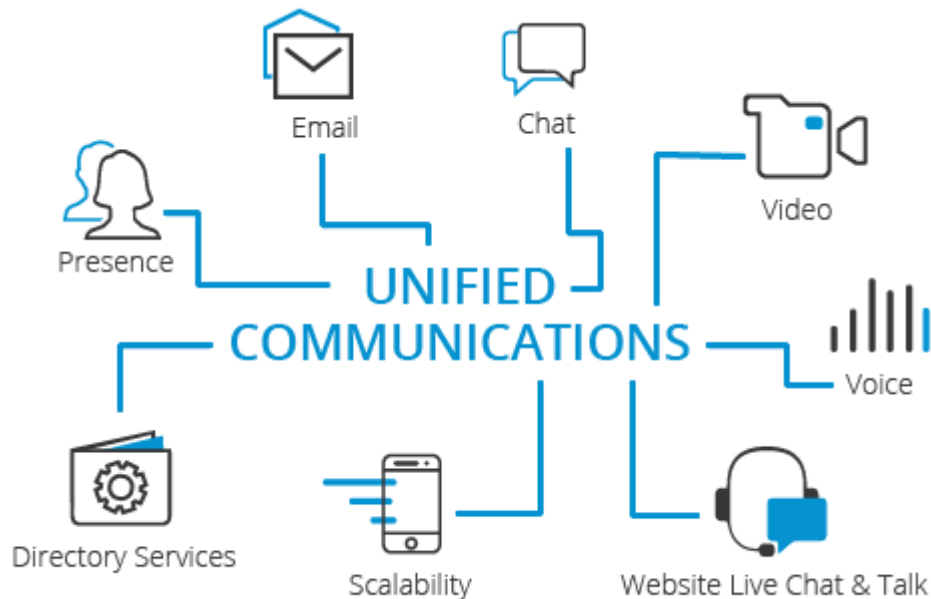


Figura 5. Comunicaciones Unificadas. Fuente: 3CX

Las empresas punteras en este campo son Cisco, Microsoft e IBM.

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 adaptarse a los medios y servicios que proporcionaban las transmisiones. Antiguamente se usaban los medios RBA (Red Básica de Área), un sistema en el que se “tiraba” un teléfono al general y se prolongaba la línea hasta otro puesto de mando. Luego se realizaba lo mismo con los medios satélite y por último un tercer teléfono para conectarlo a la Red Conjunta de Telecomunicaciones (RCT), que era la red interna de los cuarteles, ya que siempre había una toma en los campos de maniobras o poder conectarla a la red terrestre de la ciudad en la que se estuviese. Evidentemente tres teléfonos con tres extensiones diferentes para el general podría ser una pérdida de eficiencia. De esta manera actualmente, se está implementando el uso de los CM debido a la cantidad de medios de transmisión que hay. Con este elemento se puede centralizar los servicios de tal manera que se integre en la red el CM y así tener que poner un solo teléfono.

3.5 VENTAJAS DE LA VoIP

En este subcapítulo se verán las ventajas de la VoIP y así entender por qué los CM se están desarrollando tan deprisa. En el ejército se está llevando a cabo una transformación hacia la VoIP de suma importancia con varios aspectos a tener en cuenta:

Reducción de costes:

- Reducción del precio en el alquiler de líneas
- Reducción de precios de los equipos de red de datos y supresión de la necesidad de adquirir equipamiento telefónico.
- Reducción de costes de mantenimiento, menos equipos y menos personal para



mantenerlo.

La eficacia en el encaminamiento de la información es evidente. Esto es debido al uso del enrutamiento dinámico o automático propio de las redes de internet. Con la VoIP en un puesto de mando, el jefe podrá hacer uso del terminal sin preocuparse de que ocurre en la línea. Antiguamente con la RBA si caía un medio la línea se volvía inútil, pero actualmente con esta implementación, el CM puede enrutar si no lo hace un router puesto a tal fin, permitiendo que, si cae un medio de transmisión, la línea siga funcionando gracias a ese enrutamiento dinámico.

En la figura 6 se aprecia la comparativa de coste el minuto y de establecimiento de llamada entre una llamada analógica y otra digital una vez implementada la centralita en la red [5].

	VoIP	Telefonía analógica
Precio medio de fijo a móvil	0,02€/min	0,25€/min
Establecimiento medio de llamada	0 €	0,18 €

* Enero de 2020

Figura 6. Costes. Fuente: Sarennet

Desarrollo y provisión de servicios de valor añadido:

- Mensajería unificada: correo electrónico junto con aplicación de voz.
- Soporte de aplicaciones multimedia tales como videoconferencia, streaming de video, carpetas compartidas, entre otros.
- Soluciones de comercio electrónico para empresas.

Implementación de servicios propios que antes eran ofrecidos por el proveedor de servicios:

- Identificación de llamadas.
- Servicio de llamada en espera.
- Transferencia de llamadas.
- Llamada a tres.
- Devolver última llamada.
- Repetición de llamada.



- Mostrar mensaje de fuera de servicio.
- Envío de llamadas al buzón de voz.

Sin duda la reducción de costes es la mayor ventaja. Pero como se ha podido ver hay una cantidad de ventajas secundarias para tener en cuenta, por no hablar de la sencillez en la escalabilidad que permite la VoIP muy útil para empresas y organismos como para el Ejército de Tierra.

4 DESCRIPCIÓN ASPECTOS TECNOLÓGICOS

En este capítulo se va a hablar sobre los diferentes tipos de protocolos con los que se trabaja no solo en los CM, sino en los equipos que están inmersos en las redes IP. A parte se nombrará y explicará lo que es un códec. De esta manera se pretende ahondar en dos conceptos básicos para entender cómo se comporta un CM y por qué luego puede haber problemas de tráfico o configuración al haber conflictos de entendimiento entre un terminal y otro si no usan el mismo protocolo o códec.

4.1 PROTOCOLOS DE SEÑALIZACIÓN

Protocolo: Es el 'lenguaje' que se utiliza para negociar y establecer las comunicaciones de voz sobre IP. Los más importantes: SIP, H323, IAX2, MGCP.

En los últimos años, los protocolos de señalización para el servicio de voz han evolucionado desde el transporte analógico por conmutación de circuitos a la digital por conmutación de paquetes.

Los estándares que rigen estos protocolos han ido adaptando el proceso de análisis cuantificación y compresión para ir mejorando la calidad del servicio. Esta tendencia ira evolucionando a mejor según pase el tiempo y se vayan mejorando los anchos de banda y la infraestructura y equipos en general. Haciendo que empresas y organismos mejoren su eficiencia gracias a estos estándares.

En los siguientes puntos se van a analizar los estándares para VoIP (H.323, SIP, SCCP y MGCP) que son los usados para la señalización. Pero previamente se va a comentar brevemente como es el mecanismo de señalización en las redes telefónicas analógicas para entender esta evolución.

El significado de proxy es aquí definido para entender y continuar con los conocimientos básicos de las telecomunicaciones y redes.

El anglicismo proxy (plural proxies) o servidor proxy, adaptado al español como proxi en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética



máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc. Dependiendo del contexto, la intermediación que realiza el proxy puede ser considerada por los usuarios, administradores o proveedores como legítima o delictiva y su uso es frecuentemente discutido.

4.2 SEÑALIZACIÓN EN REDES TELEFÓNICAS ANALÓGICAS

Durante el siglo XX, la señalización sobre redes de conmutación de circuitos evolucionó debido a la expansión de las telecomunicaciones durante la primera mitad de siglo.

El sistema se basaba en la interconexión de diferentes centrales analógicas que trataban las señales y las enviaban a impulsos.

El sistema utilizado fue el sistema de señalización de red denominado Sistema de Señalización por canal común numero 7 o Common Channel Signaling System (SS7 según la ITU).

SS7 es una arquitectura de protocolos de señalización completa en la que la formación se transporta mediante mensajes. SS7 constituye un estándar global para las telecomunicaciones en redes centrales de circuitos conmutados transmitidos por canales digitales. Define los procedimientos y protocolos para el intercambio de la información en una red de señalización ya sea fija o móvil para su supervisión, control, acceso a bases de datos, gestión y enrutamiento tanto de voz como de datos. Básicamente se encarga del establecimiento de una llamada, intercambiándose información con el usuario y enrutando la llamada. En la figura 7 se ve cómo se realiza una señalización básica usando troncales entre centrales, en el Ejército se denominan E1 [6].

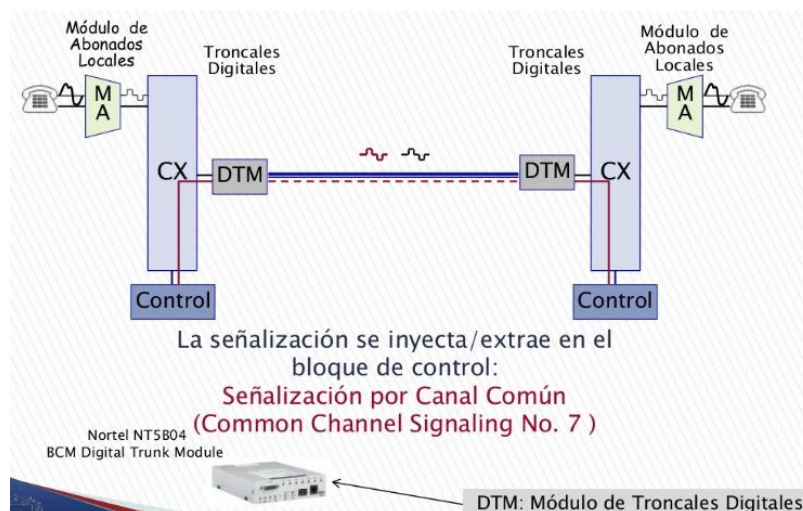


Figura 7. SS7 arquitectura. Fuente: Univ. Cauca



4.3 H.323

Es un estándar creado por el grupo de estudio 16 de la ITU-T en 1996 que describe las especificaciones para la transmisión de voz, video y datos multimedia a través de una misma red de conmutación de paquetes. Este protocolo se adoptó en el momento en el que las infraestructuras requerían datos y voz al mismo tiempo. Con este protocolo se reducía la necesidad de cables. En este estándar se definen los componentes involucrados, así como los flujos de información. Es un protocolo punto a punto en el que los puntos finales inician las sesiones. Hay que añadir que es un protocolo complejo y binario, difícil de tratar para los operadores. En la figura 7 se aprecia como el protocolo H.323 es usado por los terminales, servidor y Gateway.

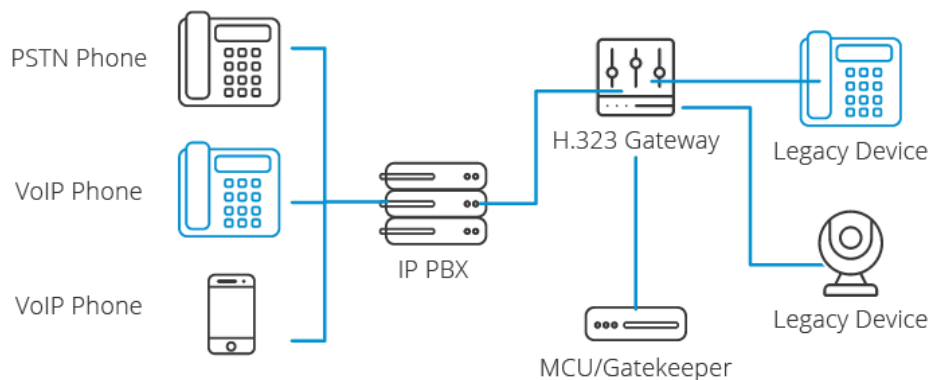


Figura 8. Uso del protocolo H.323 entre terminales. Fuente: 3CX

El protocolo H.323 en cuanto a arquitectura está compuesto por 4 dispositivos que permiten comunicación multimedia punto a punto y punto a multipunto, véase:

- Terminales H.323: ya sea un PC o un teléfono, permite la comunicación en tiempo real bidireccional.
- Pasarela H.323 (Gateway): Elemento de la red que permite la interoperación entre los terminales de la red y otras redes que no sean H323.
- Unidad de control multipunto (MCU): Elemento funcional de la red H.323 que permite las comunicaciones multipunto. Compuesto de dos partes, una negociadora denominada controlador multipunto, y el procesador multipunto que hace de mezcla de medios. Un terminal puede tener integrada la función de una MCU.
- El GateKeeper (GK): es el elemento más importante de la red, ya que proporciona servicios al resto de elementos de la red H.323, entre sus funciones destacan las de mantener el registro de los puntos finales, control de admisión, servicios de directorio o traducir y relacionar el número con la dirección IP, control del ancho de banda y filtrar y dirigir las llamadas.

Ventajas

- Implementa QoS de forma interna.
- Más completo: control de conferencias, recursos ...
- Soporta conferencias de forma nativa de vídeo y datos.



En la figura 8 se aprecia una arquitectura básica de elementos en una red VoIP [7].

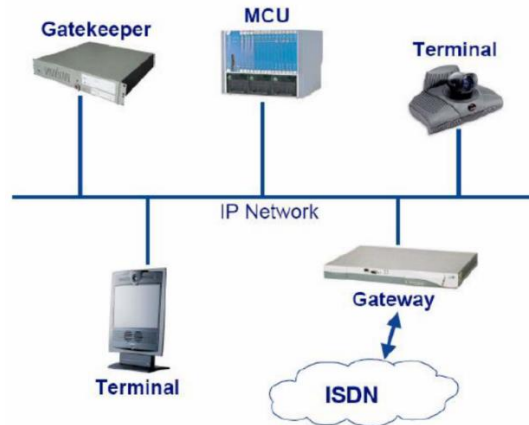


Figura 9. Ejemplo de arquitectura basada en H.323. Fuente: Server VoIP

4.4 SIP (Session Initiation Protocol)

SIP es un protocolo de señalización de la capa de aplicación desarrollado para crear, modificar y terminar sesiones multimedia entre uno o varios participantes en redes IP, soportando mecanismos de establecimiento, modificación y finalización de llamadas.

Uno de los objetivos de sus creadores fue desarrollar soluciones para el soporte de conferencias. Desarrollaron mecanismos para informar a los usuarios acerca de las sesiones existentes en la red, requisitos de medios, direcciones, etc. Existen dos modos básicos de identificar y participar en las sesiones multimedia, el mecanismo de anuncio y el de invitación.

Al igual que H.323 SIP se enfrenta a interconectar terminales y servidores con diferentes capacidades.

A diferencia de H.323, SIP utiliza cabeceras de gran longitud codificadas en texto plano que permite solucionar problemas más rápido debido a su simpleza [8].

4.4.1 Arquitectura de SIP

SIP utiliza un modelo cliente/servidor en el que los dispositivos son denominados nodos. Cualquier nodo puede comunicarse con otro. La configuración más habitual es conectar los terminales a un nodo que hace de servidor como un CM donde estos terminales se registran. Así pues, los elementos funcionales son:

- Agentes de Usuario (UA): Los agentes de usuario son aplicaciones que residen dentro del nodo SIP. Aquí se implementa el transporte sobre TCP y UDP. Existen dos componentes: Agentes de Usuario Clientes (UAC) que generan peticiones y los Agentes



de Usuario de Servidores (UAS), que responden a las peticiones de los anteriores.

- Servidores de señalización: existen varios tipos y se clasifican en servidores de redirección, Proxy y de registro.

Servidores de redirección: Se encarga de procesar solicitudes SIP emitidas por el terminal que origina la llamada y retornan una dirección de la parte llamada.

Servidores Proxy: es un servidor intermedio. Ejecuta diferentes programas dependiendo de quien reciba la petición funcionando como servidor desde el punto de vista del que llama o como cliente si es desde el punto de vista del servidor. No generan mensajes SIP nuevos, solo reenvían.

Servidores de registro: se encargan de registrar las direcciones SIP, en formato URL y sus direcciones IP asociadas, básicamente mapean las direcciones SIP con las IP, Los servidores Proxy acuden a este servidor.

En la figura 9 podemos ver los códecs usados en el protocolo SIP.

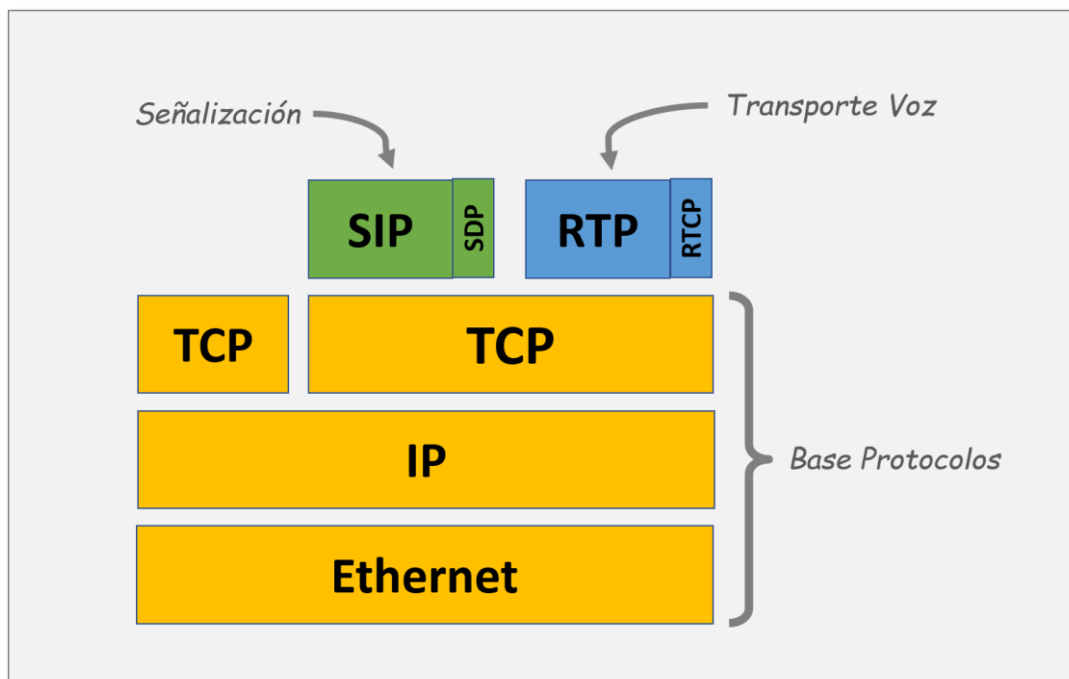


Figura 10. SIP Protocolos usados. Fuente: Vozonline.

4.4.2 Ventajas y desventajas SIP

Principales Ventajas

- Simplicidad: Basado en texto para una implementación y depuración simples, utilización de primitivas (métodos y respuestas al estilo HTTP) para establecimiento de sesiones. No se definen servicios o funciones.



- Escalabilidad y flexibilidad: Funcionalidades proxy, redirección, localización/registro pueden residir en un único servidor o en varios distribuidos.

- Simplicidad de las 'URIs' de usuario: basadas en DNS.

- No es necesario un control centralizado: funcionamiento PtP (Peer to Peer) totalmente posible ó sea es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

- SIP vs H323:

- No hay un claro vencedor.

- En EE. UU. se apostó por SIP y de ahí se ha derivado en prácticamente un estándar.

Principales Desventajas

- Problemas de Red: La utilización de un canal PtP para el streaming de audio RTP plantea numerosos problemas a nivel de red: nat routers, firewalls, ...

- Interoperabilidad con PSTN: H.323 ofrece mayores ventajas [\[9\]](#).

4.4.3 Intercambio de mensajes SIP

En la imagen se aprecia el flujo de intercambio de mensajes entre dos usuarios que pasan por una central telefónica IP.

Una sesión de llamada SIP entre 2 teléfonos es establecida como sigue:

1. El teléfono llamante envía un "invite". El "invite" lleva un mensaje SDP donde se describen, entre otras cosas, los códec de audio soportados.
2. El teléfono al que se llama envía una respuesta informativa 100 --> Tratando – retorna.
3. Cuando el teléfono al que se llama empieza a sonar una respuesta 180 --> sonando – es retornada.
4. Cuando el receptor levanta el teléfono, el teléfono al que se llama envía una respuesta 200 --> OK. El "ok" lleva un mensaje SDP donde describe entre otras cosas el códec que se utilizará en la comunicación.
5. El teléfono llamante responde con un ACK --> confirmado
6. Ahora la conversación es transmitida como datos vía RTP (Real Time Protocol)
7. Cuando la persona a la que se llama cuelga, una solicitud BYE es enviada al teléfono llamante



8. El teléfono llamante responde con un 200 --> OK.

En el caso de la figura 10 se añaden unos pasos intermedios propios de la centralita [10] [ver Anexo I y VI].

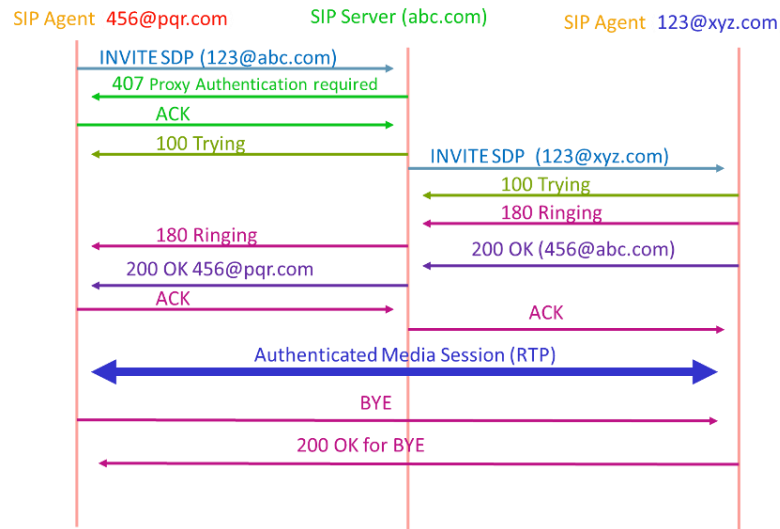


Figura 11. Flujo de llamada SIP entre extensiones IP-PBX. Fuente: 3CU electrónica

4.4.4 H.323 vs SIP

Las principales diferencias se pueden resumir en:

H.323 se presentó como una evolución de SS7, diseñado para el control de la señalización en redes de conmutación de circuitos. Por el contrario, SIP está más cercano a HTTP, empleado en Internet, paradigma de red de paquetes. De cara al futuro, es mejor decantarse por SIP.

En ambos casos, los flujos de información multimedia se transportan haciendo uso de RTP, por lo que la elección de un protocolo de control u otro no influye de manera directa en la calidad con que se ofrecen los servicios.

H.323 es mucho más complejo que SIP. Tiene cientos de mensajes diferentes codificados en binario. en SIP, por el contrario, los mensajes son de texto y muy sencillos tanto en su sintaxis como en su semántica. Por lo tanto, H3.23 complica el trabajo a los desarrolladores, así como a los administradores de redes a la hora de localizar problemas.

La arquitectura cliente/servidor de SIP es más fácil de implementar, al igual que sus mecanismos de seguridad y de gestión. H323 envía muchos mensajes a la red, con el riesgo potencial de crear congestión. Además, resulta difícil de personalizar.

SIP es más fácilmente extensible y, por lo tanto, se puede adaptar mejor a las necesidades futuras de los usuarios. H.323 presenta un mayor número de limitaciones en este sentido.

Todo el mundo coincide en afirmar que el futuro está en SIP, Los servicios en la nube basados en SIP para audioconferencia, telefonía, acceso PSTN y videoconferencia están ampliamente disponible y, por lo tanto, SIP continuará siendo el protocolo dominante para el



establecimiento y mantenimiento de sesiones multimedia en el futuro previsible. que además es empleado por IMS (IP Multimedia Subsystem). El problema es que actualmente no ha alcanzado la madurez de H.323. Por ello, hay soluciones comerciales que se basan hoy en día en H.323.

4.5 SCCP (Skinny Call Control Protocol)

Skinny Call Control Protocol o SCCP es un protocolo de control de terminal desarrollado originariamente por Selsius Corporation. Actualmente es propiedad de Cisco Systems, Inc. y se define como un conjunto de mensajes entre un cliente ligero y el CallManager. SCCP. Se utiliza para la comunicación entre Cisco Call Manager y los teléfonos Cisco VOIP. Los dispositivos de Cisco admiten principalmente estos dos protocolos, pero ejecutan SCCP de forma nativa. El Call Manager actúa como un proxy de señalización para llamadas iniciadas a través de otros protocolos como H.323, SIP, RDSI o MGCP.

Un cliente skinny utiliza TCP/IP para conectarse a los Call Managers. SCCP es un protocolo basado en estímulos y diseñado como un protocolo de comunicación para puntos finales hardware y otros sistemas, con restricciones de procesamiento y memoria significativas.

Cisco adquirió la tecnología SCCP cuando compró la empresa Selsius a finales de los años 1990. Como una reminiscencia del origen de los actuales teléfonos IP Cisco, el nombre por defecto de los teléfonos Cisco registrados en un CallManager es SEP (Selsius Ethernet Phone) seguido de su dirección MAC [\[11\]](#).

4.6 MGCP (Media Control Protocol)

Media Gateway Control Protocol (MGCP, Protocolo de Control de Puerta de Enlace de Medios o Protocolo de Control de Pasarela de Medios) es un protocolo de control de dispositivos, donde un gateway esclavo (MG, Media Gateway) es controlado por un maestro (MGC, Media Gateway Controller, también llamado Call Agent).

MGCP es un protocolo interno de voz sobre IP (VoIP) cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente – servidor.

Está compuesto por:

- un MGC, Media Gateway Controller
- uno o más MG, Media Gateway
- uno o más SG, Signaling Gateway.

Un gateway tradicional, cumple con la función de ofrecer conectividad y traducción entre dos redes diferentes e incompatibles como lo son las de conmutación de paquetes y las de conmutación de circuitos. En esta función, el gateway realiza la conversión del flujo de datos, y además realiza también la conversión de la señalización, bidireccionalmente.



El control de calidad de servicio QoS se integra en el gateway GW o en el controlador de llamadas MGC [\[12\]](#).

4.7 Protocolo IAX2

IAX (Inter-Asterisk eXchange protocol) es uno de los protocolos utilizado por Asterisk, un servidor PBX (central telefónica) de código abierto patrocinado por Digium. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de códecs y un gran número de streams, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas. Está diseñado para darle prioridad a los paquetes de voz en una red IP. Esto se llama QoS (Quality of Service).

- Creado y estandarizado por la centralita Asterisk.
- Utiliza el puerto 4569 UDP.
- Características Principales:
 - Media y señalización por el mismo flujo de datos.
 - Trunking
 - Cifrado

Ventajas

- NAT: Al enviar tanto señalización como streaming por el mismo flujo de datos (flujo UDP), se evitan los problemas derivados del NAT. No es necesario abrir rangos de puertos para RTP.
- Trunking: Es posible enviar varias conversaciones por el mismo flujo, lo cual supone un importante ahorro de ancho de banda (overhead de la capa IP y transporte UDP).

4.8 CODECS Y FACTORES A TENER EN CUENTA EN VoIP.

En este subcapítulo se explica lo que es un códec, y que factores que dependen de ellos hay que tener en cuenta en el uso de los CM y el diseño de una red.

Un códec es la forma de digitalizar la voz humana para ser enviada por las redes de datos. Algunos ejemplos: G.711, G729A, GSM, iLBC, Speex, G.723.

La transmisión de voz a través de paquetes IP conlleva problemas propios de las redes



digitales. Estos problemas se traducen en una degradación de la voz que es percibida por el usuario. Los factores tienen su relación con los códecs utilizados y dependiendo de las necesidades de la comunicación se priorizarán unos códecs u otros. Los códecs utilizados son regulados por la ITU-T.

4.8.1 Factores críticos en VoIP

Existen varios factores determinantes en el deterioro de la comunicación de voz a través de una red digital. Existen varios tipos que serán detallados brevemente de manera técnica

LATENCIA:

La latencia es el tiempo que pasa entre el envío de datos (audio en telefonía) y su recepción por el receptor. En otras palabras, en telecomunicaciones es el retraso entre el momento en que yo hablo y el que mi interlocutor escucha mi voz. Todas las etapas del transporte de la voz «digital» a través de la red de internet pueden afectar a la latencia total: Codificación y empaquetamiento de la voz, colas de espera de paquetes, número de elementos de la red por los que debe pasar el paquete (cuantos más elementos, más largo es el trayecto...), así como, la potencia de la tasa de transmisión.

Se pueden identificar problemas de latencia en telefonía IP cuando durante las conversaciones telefónicas se escuchan ecos y lagunas (cortes de conexión o pérdida de información). Otras causas se ven en la figura 11, los cuales se deberían tener en cuenta.

Problemas/ causa	Conexión internet	Códec	Sobrecarga procesos PC	Cascos	Conexión interlocutor
Cortes	☹	☹	☹		☹
Voz inaudible	☹			☹	
Voz robótica	☹		☹		
Voz lejana	☹			☹	
Voz entrecortada	☹	☹	☹		
Crepitaciones	☹				

Figura 12. Posibles causas de latencia. Fuente: Gesditel

Los operadores de VoIP usan normalmente códecs más antiguos, como, por ejemplo, G711 o G729, que son bastante sensibles a las variaciones de la velocidad de la conexión a Internet y esto provoca cortes y ruidos.

Se debe asegurar que la configuración de calidad del servicio (QoS) permite priorizar el ancho de banda para el servicio de VoIP.



Puesto que la latencia de la conexión a internet se mide en milisegundos, una buena latencia para la comunicación VoIP debe ser de 60 ms o menor si se puede.

Si la latencia normal internet debe ser de unos 60 ms, cualquier valor superior a este, se supondrá un problema para las comunicaciones, ya que afectará negativamente a la calidad de las llamadas [\[13\]](#).

JITTER:

Se denomina jitter o fluctuación del retardo a la variabilidad temporal durante el envío de señales digitales, una ligera desviación de la exactitud de la señal de reloj. El jitter suele considerarse como una señal de ruido no deseada. Esto puede afectar tanto a la amplitud como a la frecuencia y la situación de fase. El jitter es la primera consecuencia de un retraso de la señal. La representación espectral de las variaciones temporales se denomina ruido de fase.

En las telecomunicaciones también se denomina jitter a la variabilidad del tiempo de ejecución de los paquetes. Este efecto es especialmente molesto en aplicaciones multimedia en Internet como radio por Internet o telefonía IP, ya que provoca que algunos paquetes lleguen demasiado pronto o tarde para poder entregarlos a tiempo. El efecto puede reducirse con un búfer de jitter, un búfer de datos, pero a costa de un tiempo de ejecución mayor. O mediante técnicas de QoS [\[14\]](#).

PÉRDIDA DE PAQUETES:

Para la comunicación en tiempo real, el protocolo de transporte UDP es el más favorable. El protocolo UDP se utiliza para transmitir voz mediante el IP, puesto que tiene la ventaja de utilizar menos tara y depende menos de protocolos de capa superior (como RTPC/RTP) para proporcionar control de errores o de flujo, o cuando «las necesidades de tiempo real» hacen que la transmisión, tal como la utiliza el protocolo TCP, sea inadecuada.

La tasa de pérdida de paquetes dependerá de la calidad de las líneas utilizadas y del dimensionamiento de la red. Para que la calidad vocal sea aceptable, dicha tasa de pérdida de paquetes ha de ser menor que el 20%.

El códec utilizado también influye a la hora de corregir las pérdidas de paquetes.

ECO:

El eco es un factor molesto que se produce cuando la señal de los altavoces entra por el micrófono de nuevo. Esto provoca una repetición de la voz y sensación de retardo.

Este fenómeno afecta más a la VoIP que a la tradicional. Un eco menor que 50 ms es imperceptible. Por encima de este valor, el hablante oirá su propia voz después de haber hablado. Si se desea ofrecer un servicio de telefonía IP, las pasarelas tendrán que procesar el eco generado por la transferencia de dos a cuatro hilos, de lo contrario, no será posible utilizar



el servicio con equipos analógicos clásicos. Como solución, se están instalando compensadores de eco de alta calidad en la pasarela de la red [\[15\]](#).

4.8.2 Mecanismos de corrección

Para evitar estos factores se usan una serie de herramientas tales:

CLASIFICACIÓN DE PAQUETES:

Para clasificar los paquetes se puede optar por marcar estos en origen en la capa 2 donde hay ampos para este fin. En el campo User Priority de la 802.1p dentro del encabezado 802.1Q. En la capa 3 en el apartado Type of Service se puede indicar como Servicio Diferenciado para mejorar la prioridad.

COLAS:

En los switches o CM se pueden usar colas priorizando el tráfico más necesario y haciendo que se pierda el menor número de paquetes.

RESERVA DE RECURSOS:

La reserva de recursos consiste en que los terminales hablen entre sí, para saber cuánto van a consumir y mantener un mínimo ancho de banda para este fin. Se denomina reserva dinámica ya que se hace automáticamente, RSVP. Se puede hacer de manera fija configurando el CM.

4.8.3 CÓDECS

Como se dijo con anterioridad al principio del trabajo, es necesario para transmitir la voz a través de una red IP, digitalizar. El proceso de digitalización de una señal analógica como es nuestra voz se hace a través de un codificador-decodificador. Códec.

Existen varias formas de codificar, pero la mayoría se basa en la modulación codificada por pulsos (PCM). Los códecs más utilizados son los de la siguiente figura 12.



Codec	Bitrate (kb/s)	Frame (ms)	Bits per frame	Algorithmic delay ^a (ms)	Codec delay ^b (ms)	Compression type	Complexity (MIPS) ^c	MOS
<i>Narrowband codecs</i>								
G.711	64	0.125	8	0.125	0.25	PCM	≪1	4.1 ^d
G.723.1	6.3	30	189	37.5	67.5	MP-MLQ	≪18	3.8
G.723.1	5.3	30	159	37.5	67.5	ACELP	≪18	3.6
G.726	16	0.125	2	0.125	0.25	ADPCM	≈1	–
G.726	24	0.125	3	0.125	0.25	ADPCM	≈1	3.5
G.726	32	0.125	4	0.125	0.25	ADPCM	≈1	4.1
G.728	16	0.625	10	0.625	1.25	LD-CELP	≈30	3.61
G.729	8	10	80	15	25	CS-ACELP	≪20	3.92
G.729A	8	10	80	15	25	CS-ACELP	≪11	3.7
G.729D	6.4	10	64	15	25	CS-ACELP	<20	3.8
G.729E	11.8	10	118	15	25	CS-ACELP LPC	<30	4
GSM-FR	13	20	260	20	40	RPE-LTP	≈4.5	3.6
GSM-HR	5.6	20	112	24.4	44.4	VSELP	≈30	3.5
GSM-EFR	12.2	20	244	20	40	ACELP	≈20	4.1
AMR-NB	4.75–12.2	20	95–244	25	45	ACELP	15–20	3.5–4.1
iLBC	13.33	30	400	40	60	LPC	18	3.8
iLBC	15.2	20	304	25	40	LPC	15	3.9
Speex (NB)	2.15–24.6	20	43–492	30	50	CELP	8–25	2.8–4.2
BV16	16	5	80	5	10	TSNFC	12	4
<i>Broadband codecs</i>								
G.722	48, 56, 64	0.0625	3–4	1.5	1.5625	SB-ADPCM	5	~4.1
G.722.1	24, 32	20	480, 640	40	60	MLT	<15	~4
AMR-WB (G.722.2)	6.6–23.85	20	132–477	25	45	ACELP	≈38	Various
Speex (WB)	4–44.2	20	80–884	34	50	CELP	8–25	Various
iSAC	Variable	Adaptive	Adaptive-variable	Frame + 3 ms	Adaptive	Transform coding	6–10	Various ^e
BV32	32	5	160	5	10	TSNFC	17.5	~4.1

Figura 13: Códecs VoIP. Fuente: Sip Systems

En la tabla se observa la velocidad de transmisión en la primera columna, en la segunda y tercera indica la velocidad de transmisión de imágenes (fotogramas) y la cantidad de bits que consumiría en caso de videollamada, la cuarta y quinta el retraso en ms, la sexta el tipo de algoritmo utilizado en su compresión, la penúltima columna habla de la complejidad a la hora de codificar el lenguaje, y por ultimo un estándar que habla de lo bueno que es el códec después de su codificación-decodificación en un rango de 1 a 5 siendo 1 el más pobre y el 5 el mejor [16].

El proceso de codificación se realiza en tres pasos básicos:

Muestreo:

Definimos muestreo como la cantidad de veces que medimos el valor de la señal en un periodo de tiempo (usualmente en 1 segundo). Según el teorema de Nyquist-Shannon la cantidad de veces que debemos medir una señal para no perder información debe de ser al menos el doble de la frecuencia máxima que alcanza dicha señal.

En otras palabras, si deseamos grabar una conversación telefónica, como el ancho de banda de la red telefónica es de 3khz, para no perder información deberemos tomar del orden de 6.000 muestras/segundo. Como vemos en la figura 13.

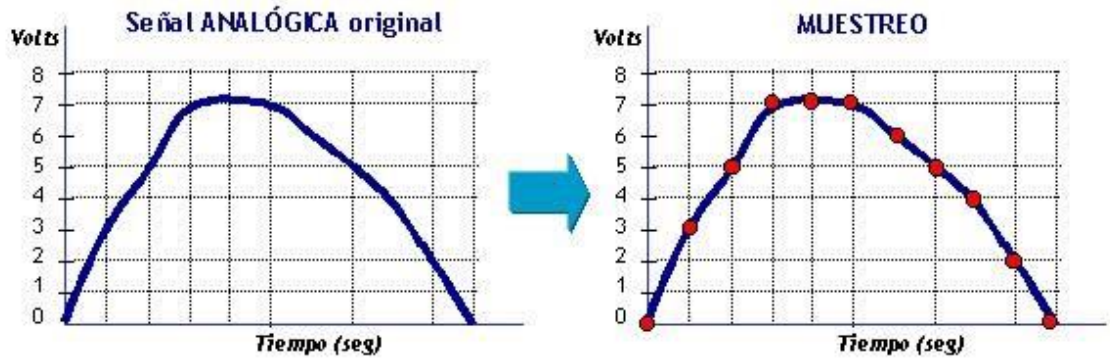


Figura 14. Muestreo. Fuente: Systemvan

Cuantificación:

En esta fase, se asigna un valor a cada una de las muestras tomadas en el paso anterior. Este valor dependerá de la precisión del sistema. Es introducido un error de aproximación generalmente. Si aumentamos el número de valores, disminuye el error. O utilizando valores no uniformes. Como vemos en la figura 14.



Figura 15. Cuantificación. Fuente: Wikiwand

Codificación:

En esta fase, se convierte los valores obtenidos de la cuantificación a código binario. Existen dos leyes, las continuas y de segmentos. El códec G.711 usa el de segmentos, por ejemplo. Muy usado en codificación de audio. Como vemos en la figura 15 [\[17\]](#).



Figura 16. Codificación. Fuente: ikastaroak

5 DESARROLLO: PRUEBAS DE CAMPO, ANÁLISIS Y RESULTADOS

En este capítulo se trata de explicar las pruebas que se realizaron realmente con los equipos, tanto en el campo de maniobras con los equipos de Cisco como en la base con el sistema Asterisk. Se mostrará un esquema orientativo de la red, así como los equipos. Previamente se hace una introducción de la situación de la VoIP y los CM en la BRIPAC.

La idea fuerza de este trabajo es por tanto el ideal de la integración de toda la VoIP de la Brigada Paracaidista. Es lo que se pretende hoy en día. Pero esto conlleva una serie de retos muy difíciles.

Una de estas soluciones es la implementación de la VoIP a través de los Call Manager. Este dispositivo es un elemento vital para ello.

En los apartados anteriores se ha explicado la teoría básica para poder entender la voz sobre IP y como un CM trabaja en ese entorno de procesos, códecs y protocolos.

Sin duda, no todo depende del CM, pues es solo un dispositivo, servidor, dentro de una red IP en la que el soporte de transmisión y transporte y el resto de los medios influyen de manera muy evidente, siendo cuellos de botella a la hora de transmitir o elementos que suman en complejidad los datos tratados al usar otros protocolos o sistemas de transmisión. Teniendo estos medios intermedios como los CM que adaptarse a la red para así realizar su función de manera eficiente.

En los siguientes apartados se tratará de que medios había en la unidad, y se hará una comparativa entre un CM Cisco y otro CM tipo virtual Asterisk. Pues en esta comparativa se debe sacar una conclusión de que dispositivo sería el ideal para dar servicio a la Brigada de manera más eficiente y por extensión a cualquier Brigada del ejército.



5.1 MEDIOS EN DOTACION EN LA UNIDAD Y EJERCICIO PRACTICO

En la Brigada Paracaidista se disponía de dos Call Manager de la serie 2800 series de Cisco. En concreto el 2811. Se denominaban Águila y Buitre para distinguirlos si eran instalados en un puesto de mando principal o avanzado respectivamente. Sobre el papel ambos eran idénticos, pero el Águila tenía instaladas tarjetas de integración FXO y FXS.

Para hacerse una idea, un CM de Cisco es como router o un switch, y el CM Asterisk es un software visualizado en un ordenador cualquiera que soporte sus exigencias técnicas.

Aun siendo equipos competentes, y después de entrevistarme con los suboficiales responsables de su configuración, se llegó a la conclusión que eran demasiado antiguos para las necesidades de la unidad. Sus licencias estaban obsoletas, y su limitada capacidad para registrar teléfonos que no fuesen Cisco hacía de estos dispositivos elementos poco explotados para las necesidades que podían cubrir.

En la imagen se puede ver cómo es por detrás uno de los CM serie 2800, de la BRIPAC y como se aprecian las tarjetas de conversión FXO abajo a la izquierda y FXS arriba a la derecha.



Figura 17. Cisco CM 2811. Fuente: Propia

En el siguiente esquema de red simplificado de la maniobra en la figura 17, se ha añadido para entender el conexionado básico utilizado en una maniobra. Se aprecia la situación del CM abajo a la izquierda y su integración con el resto de la arquitectura de red. Se entiende que es orientativo, faltando elementos intermedios técnicos, pero con la idea que se pueda ver como colgarían los elementos terminales en el puesto de mando, y como habría posibilidad de redireccionar la salida de los servicios por diferentes medios, ya sea el ATQH (Estación Antequera, medio satélite), Ubiquiti (Sistema civil de radiofrecuencia militarizado añadiendo cifrador), Radio (se usaría la PR4-G gestionada por un sistema



GESCOM de gestión de flujo de tráfico) o CECOM (Centro de Comunicaciones propia de los cuarteles y bases). Teniendo una operatividad óptima con redundancia en caso de caída de uno de los medios.

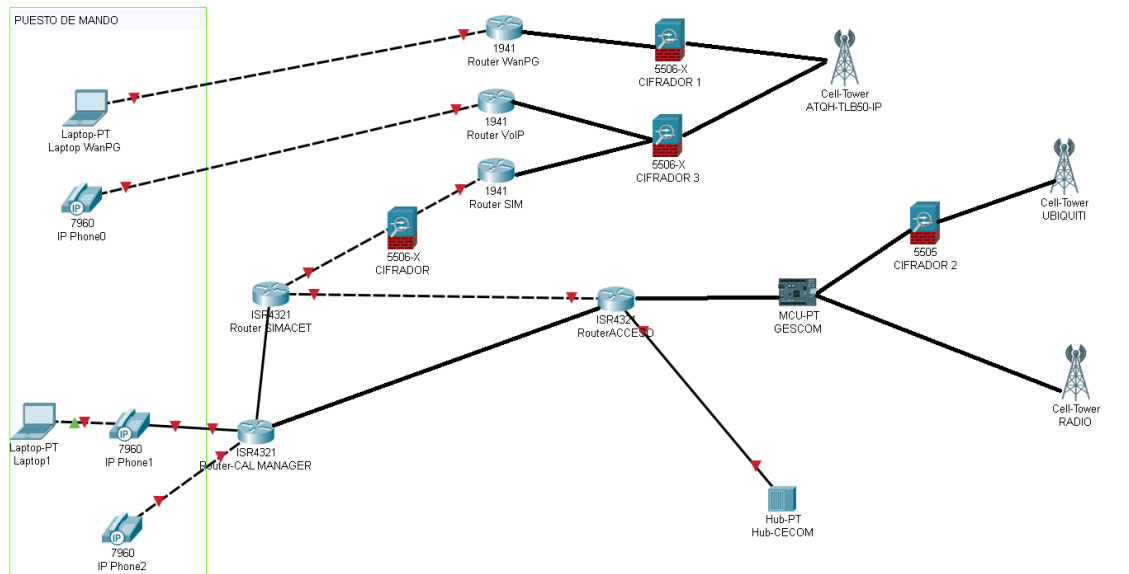


Figura 18. Esquema orientativo maniobra. Fuente: Propia

5.1.1 Requerimientos técnicos de las centrales de VoIP

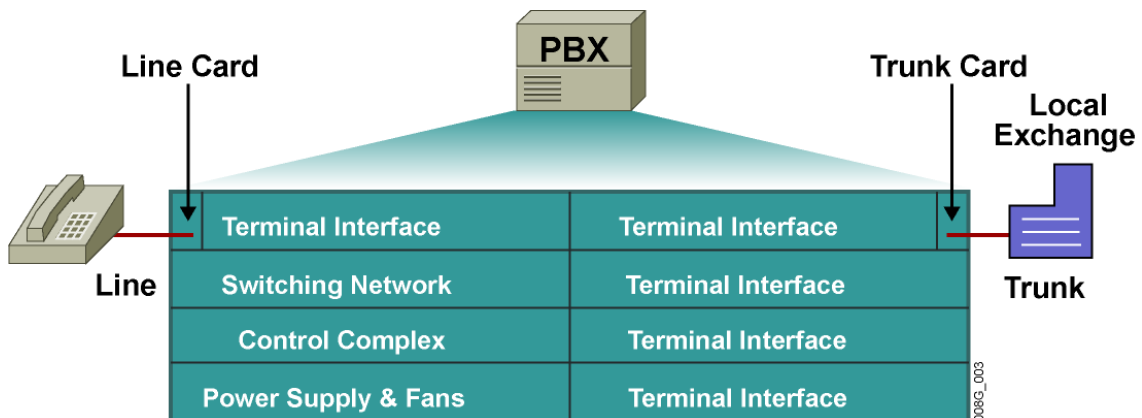


Figura 19. CM estándar. Fuente: Configuración CME ppt.

En la figura 19 se observa en forma de esquema la conexión de un terminal y la salida de un troncal desde una central IP.

En este subcapítulo se expondrán las diferentes pruebas realizadas durante las prácticas externas, en concreto en las maniobras y los aspectos técnicos más importantes de un CM con el fin de entender su análisis.

ANCHO DE BANDA: es el problema diario en un técnico de telecomunicaciones en el ejército. Es el embudo por donde todo pasa y el que limita los servicios. El que hace que un jefe



de centro de transmisiones tenga que ponerse a pensar que servicio es prioritario y que medios debe llevarse para poder realizar la misión encomendada.

Debido a las características de los medios, y al terreno, el ancho de banda suele ser insuficiente, por eso es importante elegir una central adecuada. Si bien es el medio de transmisión y no la central el que limita el ancho se debe tener en cuenta estos medios.

- Radioenlaces a través de antena Ubiquiti con enlaces de hasta 100Mbps o más, pero limitando el alcance a 20 kms, teniendo que usar repetidores para prolongar la línea, y dan muchos problemas de enlace porque son direccionales. Se ha solucionado creando antenas multidireccionales puestas en los puestos de mando que pueden recoger varias señales a la vez de otras Ubiquitis.
- Enlace satélite, con estaciones ATQH y TLB50-IP a 2 Mbps retrofitados a 10Mbps gracias a sus módems actualizados, o con la estación Soria (SOTM Satellite On The Move) a 128Kbps con distancia global.
- Radioenlace, su bien con las radios HF de Harris es imposible conectar los CM pues la tasa es demasiado pequeña, con la PR4-G si se ha podido usando los gestores VMI de las estaciones Mercurio 2000. El alcance es de 10 kms sin usar radioenlaces y en condiciones óptimas con velocidades de 128Kbps en modo Supermux.
- Enlace con dispositivos 4G con tarjeta civil contratada, y prolongación por línea UTP o fibra. Con alcance de 100metros si fuese UTP y hasta 4 kms empalmando bobinas de 1 km. Podría ser más, pero no hay tantas bobinas por dotación. La velocidad puede ser de 100Mbps hasta 600Mbps dependiendo de lo contratado.

Por supuesto estas velocidades son aparte de VoIP para otros servicios en uso en el puesto de mando, como el Sistema de Mando y Control del Ejército de Tierra (SIMACET), mensajería, o de los nodos que contienen los servicios propios y su réplica a otros puestos de mando.

Dentro de la propia llamada el que determina el ancho a consumir en el códec usado para tal fin. En los ejercicios realizados se usó el G.729^a pues al usar una compresión más efectiva, ocupaba solo 8Kbps. Aunque dependiendo de la central a usar, el CM de Asterisk usaba SIP y el CM de Cisco usa el SCCP. El uso de diferentes códecs hace que al final el consumo de recursos sea ligeramente mayor a las especificaciones técnicas.

Las practicas realizadas fueron para un ejercicio tipo EPCIS, Ejercicio Practico CIS, de octubre de 2022 en el campo de maniobras de Uceda de la BRIPAC. En este escenario se realizaron diversas practicas por parte de las secciones orgánicas, permitiéndome realizar una práctica de prueba de centrales, conectando las dos centrales Cisco serie 2811. En estas se conectó un teléfono cisco en cada central para ver cómo se registraba automáticamente una vez configurados los CM. A la vuelta de maniobras y con la ayuda de un Sargento de Transmisiones, se realizaron pruebas con Asterisk usando dos ordenadores, uno como central y otro como shoftphone, o teléfono virtualizado.



SEGURIDAD: Dentro del Ejército en cuanto al trato de la información es uno de los factores más importantes. A priori siempre será más segura una central de código cerrado como el CM de Cisco frente al código abierto de Asterisk, y esto es así porque Cisco es muy celosa con sus terminales y el posible robo mediante espionaje industrial, haciendo equipos muy seguros y capados a la hora de su optimización, o configuración. Teniendo que pagar licencias periódicamente a cuál más cara, mejorando su acceso según se va pagando más y más.

A parte, la seguridad siempre está reñida con la operatividad, y en la unidad en la que hice las prácticas, y atendiendo siempre a los consejos de mi tutor militar el Capitán jefe de la CIA de Transmisiones, Don Miguel García Montero, este me comentó esta dualidad entre la seguridad y la operatividad.

En una unidad como la BRIPAC, que es de carácter expedicionario, quiere decirse, que es la primera en entrar, muy detrás de las líneas enemigas, rodeado de terreno hostil, la velocidad, y el tiempo, juegan siempre en contra. Esto quiere decir, que, a la hora de instalar un puesto de mando, solo se tendrías de 24 a 72 horas como máximo que es lo que duraría la misión antes de ser relevada. En este tiempo, las transmisiones han de montarse a contrarreloj, sin tiempo de certificar la seguridad por entidades externas. Por lo que el uso de un CM lo más securizado posible es vital. Bien es cierto que existen los cifradores. Pero en esta unidad que todo ha de lanzarse en paracaídas, un cifrador de más, cuenta. Por lo que a la hora de elegir un CM Cisco o Asterisk es importante cual es más seguro. Así pues, el capitán me abrió los ojos que el adaptarse y ser flexible es vital pero posible. Por otro lado, el Sargento de Transmisiones Don Víctor Morcillo Scholl, en otra de las entrevistas que tuve, se decantaba por los CM de Cisco por este motivo entre otros.

A parte de esta seguridad, hay que tener en cuenta la seguridad en dos aspectos.

1. Desde el Centro de Transmisiones (CT) al Puesto de Mando (CP Comand Post): ambos centros están relativamente cercanos dentro de una zona acotada por alambrada, parapetos, sacos terreros, etc. Con accesos controlados por la Policía Militar (PM). Se puede hacer uso de cable UTP si están a menos de 100 metros o fibra óptica (FO) si, es más. No sería necesario cifrar las cosas en esta burbuja hasta no ser mandadas a la zona Hertziana para su salida al mundo.

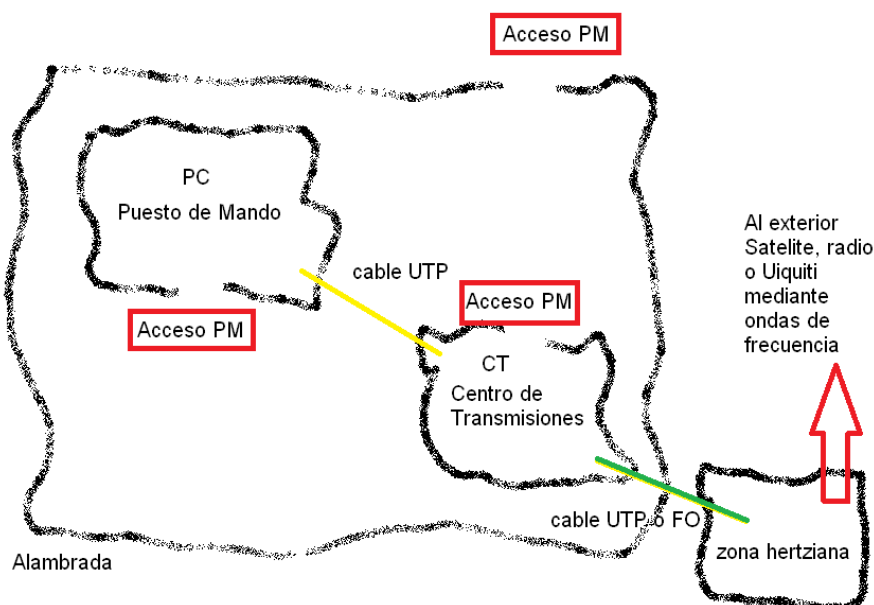


Figura 20 Esquema de un Centro de Transmisiones

- Del Centro de Transmisiones a otro Centro de Transmisiones. Este enlace abarcaría desde los 10kms a la distancia necesaria para enlazar por ejemplo con Afganistán a más de 6000kms. Para ello el ejercito dispone de los siguientes cifradores dependiendo de los medios a utilizar como vemos en la Tabla 1.

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

Tabla 1. Tipos de Cifradores. Fuente: MinisDef

Como podemos deducir, la parte negra o cifrada del circuito sería proporcionada por estos cifradores, que son utilizados como elementos en serie de la cadena de transmisión, a poder ser, casi el último elemento justo antes de la antena, para poder trabajar con la información en rojo o en claro dentro de la estación o usarla por parte de los mandos en el puesto de mando.

5.2 GESTIÓN DE LAS CENTRALES

Este subcapítulo tiene como objetivo mostrar la diferencia entre la gestión de una y otra central.

Teniendo en cuenta que la BRIPAC da servicio a su Cuartel General para la dirección y control de las unidades de la Brigada, por ello la Compañía de Transmisiones está encuadrada en el Batallón de Cuartel General, dando servicio a entidad de Brigada para abajo, si bien realiza ejercicios con todas las unidades de España. Como se puede ver en la figura 21, la CIATRANSPAC o Compañía de Transmisiones, sale del Batallón de Cuartel General, del que forma parte y aporta casi el 50% de su personal.

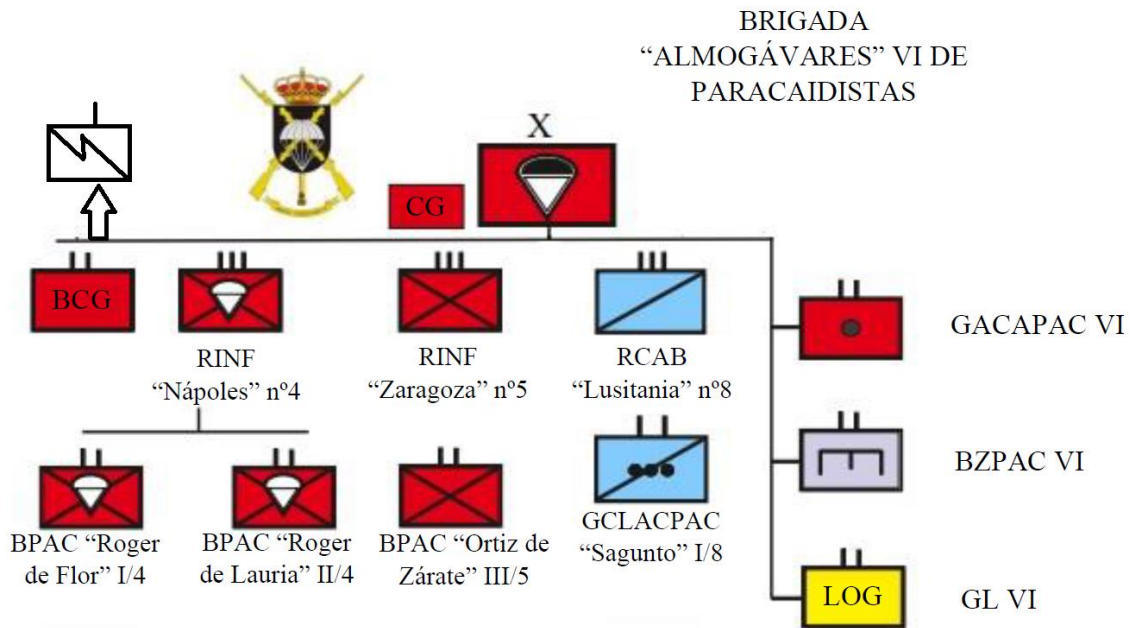


Figura 21. Organigrama BRIPAC. Fuente: Propia

Desde el Puesto de Mando de la Brigada se controlarían hasta 2000 personas si se desplegara entera. Aunque lo normal son cifras inferiores por el carácter expedicionario de la Unidad, la primera en abrir brecha en cualquier misión u operación. Sin la Compañía de Transmisiones, no podría dirigirse esta Unidad de elite del Ejército de Tierra. Tanto es así, que en la nueva organización del Ejército, esta unidad comparte división con el Mando de Operaciones Especiales, el Mando de Tropas de Montaña, y las Fuerzas Aeromóviles del Ejército de Tierra, queriendo decir con esto, que forman parte del selecto grupo de unidades especiales de nuestras Fuerzas Armadas. Es por esto por lo que la exigencia de excelencia en la Compañía de Transmisiones es muy alta. Cabe mencionar la obligación del curso paracaidista una vez destinado en esta unidad.

La dependencia directa es de la División San Marcial que acoge las unidades anteriormente descritas. Como se puede ver en el extracto del BOD la figura 20 muestra la nueva organización del Ejército que de 2020 [ver Anexo VII].

Con esto se deduce que normalmente el número de clientes de la Brigada serán limitados y por ello, las centrales para tener en cuenta y su configuración deben ser acordes para optimizar al máximo los recursos. Así pues, su configuración variará de una a otra.

ASTERISK:

1. Lo primero para tener en cuenta es la creación de un servidor donde albergar la máquina virtual. A ser preferible un ordenador con una potencia suficiente para poder tener dedicado una máquina a este servidor, y luego crear si es necesario en el mismo ordenador máquinas con teléfonos virtuales.
2. Una vez creado el servidor que gestionará el CM, hay que crear las extensiones de los



números de teléfono que se van a colocar.

3. Asociar cada extensión a una dirección IP.
4. Realizar los troncales con el resto de los Puestos de Mando.
5. Categorizar el teléfono.

El trabajo de configuración se realiza en el cuartel, denominado maqueta, una o dos semanas antes de salir al campo de maniobras. En el momento del despliegue solo se debe montar los equipos, aunque la realidad demuestra que a veces se deben hacer ajustes de última hora.

CALL MANAGER DE CISCO:

El CM de Cisco destaca en que su configuración puede quedar guardada para diferentes ejercicios si estos se parecen, pues su sistema sencillo hace que solo se deban conectar teléfonos para registrarlos en él. Pero bien es cierto que es mejor realizar una configuración para cada maniobra para ajustar sus capacidades. Lo importante en este tipo de CM es tener las licencias a punto y los teléfonos Cisco compatibles con el CM, pues los teléfonos Mainstream de código abierto no se registrarán. Uno de los inconvenientes de esta centralita. También es importante que los teléfonos tengan el firmware acorde a la central o al menos tener los archivos de firmware para poder instalarlos en el CM.

COMPARATIVA DE GESTIÓN entre Cisco vs Asterisk

A priori la gestión del Asterisk es más amigable pues se realiza con una muestra de los parámetros en una pantalla más amigable a través de una dirección web, en cambio la de Cisco parece menos accesible pues se realiza a través de comandos. De todos modos, los comandos de Cisco son los estándares, y son comandos conocidos por el personal de Transmisiones, no así el uso del Display de Asterisk, pues hace falta una guía para asegurar que comandos son importantes a la hora de configurar.

Se ha hecho una captura de pantalla mientras se configuraba el CM de Cisco para apreciar su modo de presentar la información, cosa que se observa en la figura 22.

En la figura 23 en cambio se muestra una captura de un momento en el proceso de configuración de una centralita Asterisk, la Tripbox.

Se aprecia claramente como Cisco se basa en comandos y Asterisk se basa en pestañas interactivas.

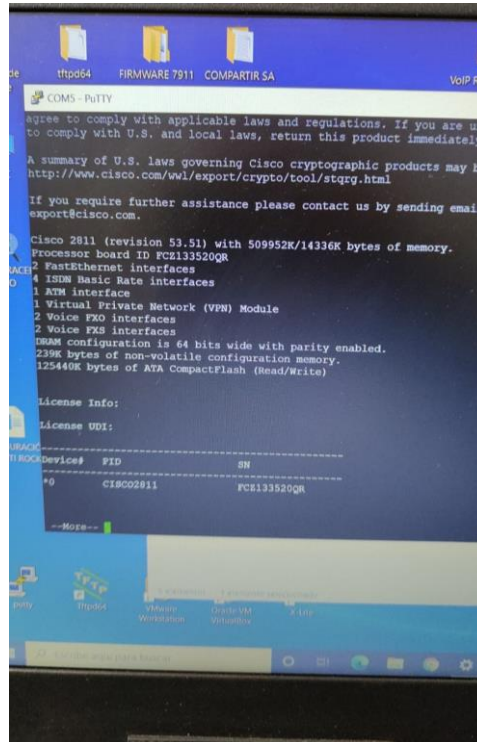


Figura 22. Línea de comandos en CM Cisco. Fuente: Propia

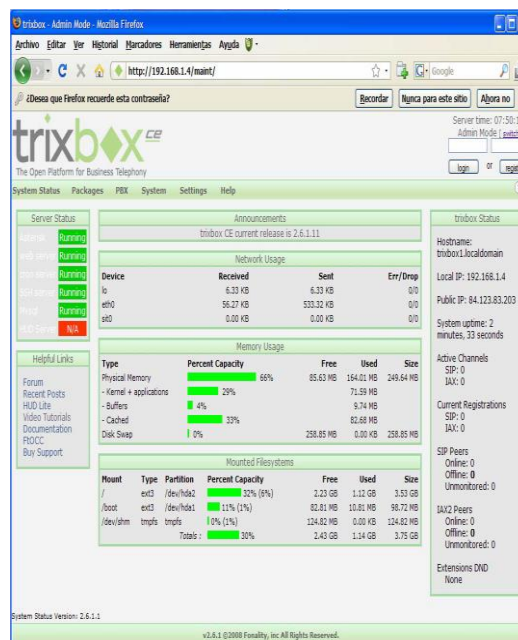


Figura 23. Configuración CM Asterisk Trippox. Fuente: Propia

Debido a que los CM que están integrados en la estación ATQH son imposibles de acceder ya que los configura CGES, se hace necesario el uso de CM independientes en las unidades de



tipo Brigada, para así poder gestionar en el Centro de Transmisiones la propia central, ya que muchas veces el ATQH al ir sobre un vehículo no esté operativo, por no decir que no es lanzable hoy por hoy desde un avión. Esto demuestra la necesidad imperiosa en esta unidad en concreto y en las brigadas en general que la configuración de un CM es de vital importancia para su personal, inclusive si el número de clientes es bajo, pues su polivalencia y robustez es muy útil.

Bien es cierto que cualquier error aparecido en la maniobra se puede solventar reconfigurando el terminal, en el CM de Asterisk es más rápido por lo fácil que es seleccionar pestañas con el ratón en la pantalla, en cambio en el CM de Cisco habrá que ir configurando poco a poco de manera más lenta. Por no hablar que si hay routers implicados habrá que tocarlos también.

Por otro lado, la redundancia es vital en las transmisiones, esto quiere decir que al tener un CM virtualizado en un ordenador permite poder trasladar una imagen o snapshot del mismo y trasladarlo a otro ordenador o maquina en caso de que la primera diese problemas de funcionamiento, arranque o lentitud de procesamiento. Pero también es cierto que el Sargento Morcillo, y el Sargento Rafael Álvarez Castaño, ambos especialistas en VoIP, apuntaron en el cuestionario que el sistema que provee Asterisk es más débil en cuanto al proceso de encendido y apagado por no hablar de su inestabilidad, pues es más sensible a picos de tensión y adversidades ambientales debido a la maquina en la que son instalados [ver Anexo II y III].

En unas maniobras los efectos meteorológicos son factores muy a tener en cuenta y los equipos sufren mucho con el calor, la arena y la humedad. A parte, en los ejercicios de la BRIPAC y de las brigadas en general, la estancia en un punto determinado es muy temporal, y se realizan “saltos” de una posición a otra que requieren un encendido y apagado rápido y muy repetitivo. Aquí el CM de Cisco es el que mejor se comportaba en tiempo y estabilidad.

5.2.1 Servicios y compatibilidades

El objetivo de este apartado es comparar los servicios que puede dar cada una de las centrales, así como la contabilidad de estas con respecto a diferentes modelos de diferentes proveedores.

Asterisk

La central Asterisk como bien se referenció es una central de código abierto, esto es, que podemos ir actualizando su software gratis descargando sus actualizaciones desde internet. A parte usa el protocolo SIP, que, igual que se describió antes, es un protocolo en expansión, moderno y sencillo que trata de unificar protocolos trabajando más rápido y con menor coste de ancho de banda. Todo esto quiere decir que esta central es polivalente y compatible casi con cualquier terminal, pues si faltase algún códec o firmware, este podría añadirse a la central de manera gratuita si lo encontramos o disponemos de el en la web pertinente. El único requisito seria tener entre otros estos códecs:

En la figura 24 se observa el consumo de ancho de banda de cada códec, y como el G.729 que es el que se está imponiendo, es el más eficaz. Aunque aún se sigan usando los



anteriores en algunos equipos mientras se hace la transición y modernización en el ET.

Nombre	Estandar	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	MOS (Mean Opinion Score)
G.711	ITU-T	64	8	Muestreada	4.1
G.723.1	ITU-T	5.6/6.3	8	30	3.8-3.9
G.726	ITU-T	16/24/32/40	8	Muestreada	3.85
G.729	ITU-T	8	8	10	3.92
GSM	ETSI	13	8	22.5	3.5-3.7
Speex	-	8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	30 (NB) 34 (WB)	-
iLBC	-	15.2 / 13.3	8	20/30	4.1

Figura 24. Consumos códecs. Fuente: VoIP

Así pues, estos códecs compatibles con Asterisk permiten el enganche de un numero alto de terminales. En el ejercicio práctico realizado con la BRIPAC no fueron más de 10, pero sin duda, y corroborado por los operadores, el límite es mucho más alto, siempre atendiendo al embudo de los medios de transmisión y sus soportes.

Con el Call Manager se tuvo menos problemas de configuración por lo antes mencionado, mereciendo especial atención el hecho que los operadores aseguran que están mejor entrenados con los comandos de Cisco desde la Academia de Ingenieros del ET de Hoyo de Manzanares, cosa que yo también puedo asegurar, pues mi paso por esa academia como Sargento del arma de Transmisiones de la 42 promoción de 2014 a 2017. El empleo de comandos Cisco con la ayuda de Packet Tracer es mayor que el uso de Asterisk. Por lo visto ya lo era en esa época, como lo sigue siendo actualmente por lo que pude apreciar por estos sargentos de promociones más modernas. Así que se puede asegurar que la formación del personal en la configuración de Cisco es ligeramente mayor en esta central, a parte que tienen que configurar routers Cisco o switches de capa 3 que permiten enrutamiento, haciendo que la destreza con estos comandos sea mayor.

5.2.2 Presupuestos

Este apartado ha sido enfocado en la creación de un presupuesto aproximado y lo más actualizado posible a la adquisición y puesta en marcha de un sistema de VoIP basado en Asterisk o Cisco para la Compañía de Transmisiones de la BRIPAC.

En la tabla 2 se muestran los precios para un sistema VoIP Asterisk básico. Los precios han sido consultados en Amazon y PC Componentes, atendiendo no al terminal más económico sino al más apto, atendiendo a sus capacidades. Que soportaran los códecs y protocolos propios de la centralita, así como el ancho de banda más ajustado.



Bajo el consejo de los operadores de la Compañía de Transmisiones de la BRIPAC atendiendo a las necesidades de la unidad.

ASTERISK		
Producto	Servicio	Precio
Grandstream GXP1620 Teléfono y dispositivo VoIP	VoIP	40,77€
GATEWAY GRANDSTREAM GXW4108 Analog. FXO	Tarjeta para la integración de la red con una red analógica aparte de posibilidad de video	290,34€
GATEWAY GRANDSTREAM GXW4008 Analog. FXS	Tarjeta para la integración de la red con una red analógica	193,64€
ASUS F515EA-BQ1154W Intel Core i5-1135G7/8GB/512GB SSD/15.6"	Ordenador donde hacer correr la máquina virtual	549€
TOTAL		1073,75€
		Mas 40,77€ por cada teléfono extra

Tabla 2. Precios para sistema Asterisk. Fuente: Propia

A parte se debe proponer el uso de teléfonos con videoconferencia integrada, este tipo de medios es muy útil por parte de los generales jefes de brigada y división, si bien es cierto que se usa videoconferencias con equipos dedicados, a veces por espacio, tiempo y en el caso de la BRIPAC peso, se propone la compra de terminales con videoconferencia integrada, que soportaría bien el equipo de Asterisk mientras el medio a usar fuese cualquiera menos radio HF.

En concreto el terminal Grandstream GXV3380 - Videoteléfono IP de 16 cuentas SIP por 405€. A parte se propone también el uso de terminales IP inalámbricos permitiendo al general poder moverse por el puesto de mando o alejarse de este si es necesario de la base del terminal Grandstream Networks DP722 - Teléfono IP con un alcance de 50m hasta 350m. Muy útil si el puesto de mando es una Mula móvil, vehículo tipo lanzable de la BRIPAC



y el general no puede estar cerca de este. Precio de 88€. Por supuesto son terminales compatibles en protocolo (SIP) y códecs, incluido los de video (H.264, H.323).

En la siguiente tabla 3 observamos el precio de la adquisición de los equipos de Cisco. Los equipos elegidos han sido aconsejados por los operadores de VoIP de la Compañía de Transmisiones, a parte de la búsqueda del equipo más óptimo por precio y especificaciones a las necesidades de la BRIPAC.

CISCO		
Producto	Servicio	Precio
Teléfono Cisco CP-7821	Llamadas	111,26€
Router Cisco 4351	Central telefónica IP con licencia incluida	4751,11€
Cisco nim-2fxs/4fxop módulo de interfaz de red	Tarjeta integración red analógica	1183,81€
TOTAL		6046,16€

Tabla 3. Precios para sistema Cisco. Fuente: Propia

En la figura 26 observamos como son físicamente las tarjetas NIM FXO y FXS para un router CM Cisco 4351.



Figura 25. Tarjetas FXO, FXS para Cisco. Fuente Cisco

Para una unidad tipo brigada como es la Brigada Paracaidista “Almogávares VI” del Ejército de Tierra se ha creado un presupuesto como el de la tabla 4 y 5 para unas maniobras tipo de Brigada, con la formación de dos puestos de mando y una dotación de usuarios de telefonía de 24 personas entre los dos centros. Las necesidades serían las siguientes:



ASTERISK	<u>TELEFONOS IP</u>	<u>CENTRAL</u>	<u>TARJETA FXO</u>	<u>TARJETA FXS</u>
<u>CANTIDAD</u>	24+5 de reserva	2+1 de reserva	2+1 de reserva	2+1 de reserva
<u>PRESUPUESTO</u>	1182,29€	1647€	871,02€	580,92€
TOTAL	4281,23€			

Tabla 4. Presupuesto total sistema Asterisk. Fuente: Propia

CALL MANAGER	<u>TELÉFONOS IP</u>	<u>MÓDULO NIM</u>	<u>CENTRAL</u>
<u>CANTIDAD</u>	24+5 de reserva	2 +1 de reserva	2+1 de reserva
<u>PRESUPUESTO</u>	3226,54€	3549€	14253€
TOTAL	21028,54€		

Tabla 5. Presupuesto total sistema Cisco. Fuente: Propia

Estos resultados son los obtenidos de tener una central por cada centro (Águila y Buitre, denominación de los centros avanzado y retrasado para la BRIPAC). Y una de reserva en caso de fallo de alguna de ellas.

5.3 MATRIZ DE RIESGOS

En este subcapítulo se ha realizado un análisis de riesgo en base a la experiencia de uso y las pruebas de campo realizadas durante las practicas externas, utilizando para ello la herramienta de matriz de riesgos estudiada a lo largo del grado de Ingeniería. Esta analiza en la tabla 6 una serie de posibles causas de riesgos y daños asociados, con sus posibles correcciones y responsables. Estos datos han surgido en base a unos posibles riesgos que han ido saliendo a lo largo del uso de los mismo y la experiencia de la unidad. En la Tabla 7 se resume la cantidad de estos riesgos. Son supuestos probables, y el análisis de gravedad se deduce del grado de operatividad en los que quedaría el CM si se viese afectado por el riesgo descrito. Se aclara, que operador es el suboficial que configura y mantiene el equipo. El diseñador de la red es la oficina G6 encargada de dimensionar la red a usar en un ejercicio. El jefe es el responsable último de personal y equipo en un ejercicio, un oficial. Adquisiciones es el órgano competente para comprar los equipos a la unidad, o al Ejército dependiendo del caso.



En la tabla 1 la interpretación de los riesgos es la que sigue:

1. Riesgos bajos: No se asume ninguna acción porque se prevé su error y su funcionamiento aun con él.
2. Riesgos medios: La corrección es necesaria pero no urgente en el mismo momento. Se puede operar por tiempo limitado. Su no corrección conlleva el pase de riesgo medio a alto.
3. Riesgo alto/crítico: la corrección de este error debe ser inminente y urgente, pues la central y el conjunto de la red dejarían de funcionar.



Análisis de riesgos

Título Proyecto:		DESARROLLO DE LAS COMUNICACIONES DE VOZ IP A TRAVÉS DEL CALL MANAGER				Jefe de Proyecto:		ALBERTO PABLO GONZÁLEZ GARCÍA			Fecha cambio:	
Evaluación de riesgos												
ID	Descripción riesgo	Categoría riesgo	Causa del riesgo	Impacto (H,M,L)	Probabilidad (1,2,3)	Clase riesgo	Efectos riesgo	Medida / Alternativas	Clase riesgo tras medida	Tendencia	Responsable	Status
1	Al dar de alta x teléfonos no enruta correctamente	Desarrollo	Demasiados teléfonos	M	2	2M	No aplicable para la escala que necesito	Empleo de otro call manager	1H	(-)	Diseñador de red	Open
2	Plataforma tecnológica sin actualizaciones al día	Compras	Software desfasado o inútil	M	3	3M	Mal funcionamiento, fallos aleatorios	programa serio de actualizaciones	1L	(-)	Diseñador red, operador	Open
3	Ausencia de redundancia eléctrica	Calidad	No incorporado al Call Manager	L	1	1M	Posible caída del sistema sin SAI externa	Comprar equipo que lleve fuente extra	1L	(=)	Adquisiciones	open
4	Escenarios de pruebas funcionales deficientes	Rendimiento	Mal empleo del equipo a la hora de realizar pruebas	M	2	2M	No explotacion eficiente del sistema	aprovechar el sistema al maximo no infrausandolo	1L	(-)	Diseñador, operador	Open
5	Personal no idoneo para las capacitaciones	Cliente	Falta de formación del personal operador y montador	H	2	2H	Rendimiento deficiente del equipo	Dar cursos continuos y adecuados al personal	1H	(-)	Jefe	open
6	Desastres naturales o condiciones muy negativas	Condiciones climatológicas	Mal aislamiento del equipo en maniobras, o exceso de interperie	H	3	3H	Destrucción del equipo	Buena protección y aislamiento del equipo	2L	(-)	diseñador, operador, montador	open
7	Rotación del personal	Recursos	Mala rotación del personal	M	3	3M	Mala operacón del equipo	Suficiente personal de operación para rellenar todos los turnos	1H	(-)	diseñador	open
8	Planeamiento de costos insuficientes	Coste	Deficiencia de recursos, terminales	H	3	3H	Incumplimiento de cubrir los servicios	Aumento del gasto ajustado a las necesidades	2L	(-)	Jefe	open
9	Pérdida desmedida de información	Priorización	Mala gestión de los protocolos, QoS	L	1	1L	Posibles fallos en la llegada de paquetes IP, mala calidad de sonido	Ajustar el firmware, y alta de QoS en los terminales	1L	(-)	operador	open
10	Capacitaciones sin proceso de evaluación de conocimiento adquirido	Comunicación	Mala corrección de errores futuros	L	1	1L	Pérdida de tiempo y eficacia a la hora de explotar la red subsanando errores	Buen feedback entre operadores, apuntar errores y sus soluciones	1L	(-)	operador	open
11	Caída de conexión con otros centros	Complejidad e interfaces	Deficiencia de las tarjetas FXO/FXS	H	1	1H	Pérdida de conexión con la red CECOM, o civil	Tener tarjetas de repuesto	1L	(-)	Adquisiciones	open
12	Equipo no ruggedizado	Compras	No implementar unas protecciones suficientes para los golpes del equipo	L	3	3L	Posibilidad de rotura del equipo al transportar/lanzar en paracaídas	Rugerizar en el escalon de mantenimiento con planchas de metal y poliestireno	1L	(-)	Jefe	open

Tabla 6. Matriz de Riesgos. Fuente: Propia



Matriz riesgos proyecto						
					Estadística	
Probabilidad	3	1	2	2	Clase riesgo	Número
	2	0	2	1	Crítico	2
	1	2	1	1	Alto - medio	3
		Low	Medium	High	Medio	5
		Impacto			Bajo	0
					Total:	10

Tabla 7. Tabla de cantidad de nivel de riesgos de la Matriz de riesgos. Fuente: Propia

La interpretación de la Tabla 7 es que, los problemas relacionados con un CM suelen ser de crítico a medio no habiendo bajos, pues es un equipo crítico una vez se procede a su uso, reflejando la importancia que cae sobre él, y sus responsables.

5.4 CUADRO DAFO

En este subcapítulo se analiza la información obtenida en apartados anteriores, y se puede sintetizar en un cuadro DAFO para tener un mayor conocimiento sobre la necesidad específica de la unidad y sobre los CM. El análisis DAFO permite ordenar y sintetizar la información obtenida facilitando su empleo de una manera sencilla y rápida. La tabla 8 recoge el análisis DAFO de un CM ya sea Asterisk o Cisco, analizando sus características internas (debilidades y fortalezas) además de las externas (amenazas y oportunidades).



DEBILIDADES	AMENAZAS
<ul style="list-style-type: none"> - Equipo de inversión inicial grande. - Equipo con necesidad de atención continua en gestión ya sea por licencias u operación. 	<ul style="list-style-type: none"> - Equipo altamente tecnológico sensible al transporte y condiciones atmosféricas. - Requiere una formación continua a la par que avanza los sistemas tecnológicos.
FORTALEZAS	OPORTUNIDADES
<ul style="list-style-type: none"> - Los sistemas de telefonía VoIP son capaces, flexibles y fiables. - El sistema de telefonía VoIP permite compartir cualquier tipo de archivo mientras se está entablando conversación. - Fácil gestión y dualidad como centralita y router. 	<ul style="list-style-type: none"> - Los ahorros de costes debido a la unificación de la comunicación. - Permite nuevos servicios como llamadas calientes o directas y videollamadas.

Tabla 8. Análisis DAFO. Fuente: Propia

6 COMPARACIÓN DE LOS SISTEMAS DE VoIP

Este capítulo del trabajo ha sido enfocado en la comparación de ambos sistemas de VoIP. Para ello se recogerán los resultados obtenidos en las pruebas y conocimientos de los capítulos anteriores como presupuestos y ejercicios prácticos entre otros.

6.1 ANCHO DE BANDA

En este subcapítulo se analiza el ancho de banda consumido por una llamada de VoIP. Se ha comprobado que ambas centrales tienen un consumo de ancho de banda parecido. El ancho de banda consumido se determina por el programa Wireshark o similar de monitoreo.

Como se vería en una simulación de llamada tipo, la herramienta de monitoreo de VoIP de OpManager permite ver el consumo de ancho de banda que es de alrededor 0,1Mbps, tanto en Cisco como en Asterisk. Como puede verse en la figura 26. Superior al teórico de consumo especificado por una llamada desde un teléfono IP que asegura que con el códec G.729 sería de 8Kbps. Pero la verdad es que el consumo real es mayor debido a otros procesos de señalización, corrección y reenvío de paquetes para asegurar la calidad del



servicio (QoS).

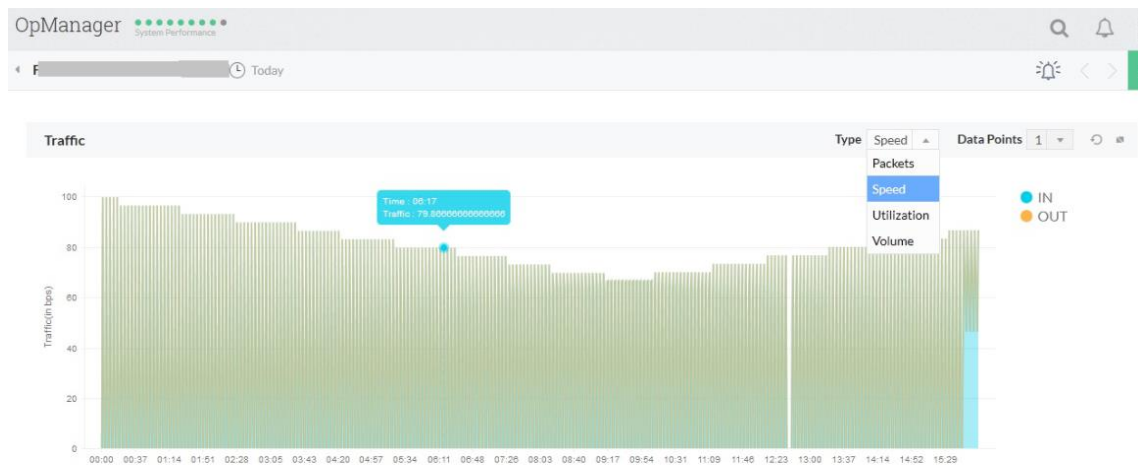


Figura 26. Consumo llamada VoIP. Fuente: OpManager

La diferencia entre una central y otra es el uso del ancho en los silencios de la llamada, donde el CM de Cisco no hace uso de este ancho durante los silencios. Esto es debido a que usa un protocolo que tiene esto en cuenta. Es el SCCP descrito anteriormente. Cuyo modo de codificación es el VBR (tasa de bits variable), es decir, adapta el ancho de banda a su utilización real. Asterisk utiliza el protocolo SIP con el modo de codificación CBR (tasa de bits constante) que envía paquetes continuamente, aunque no se esté usando la línea. Cisco sería la elegida.

6.2 SEGURIDAD

En este subcapítulo se trata la seguridad en las comunicaciones. Como se explicó anteriormente, la seguridad en las Transmisiones del Ejército de Tierra está cubierta por una serie de cifradores. Pero también se ha dicho anteriormente que, la idiosincrasia de la BRIPAC exige operaciones muy rápidas y de alta movilidad. Esto choca frontalmente con la adición de seguridad por medios tipo cifrador, con lo que la central de Cisco ofrece mejor seguridad gracias a sus licencias y software protegido.

6.3 GESTIÓN

Después de haber realizado el ejercicio práctico en las maniobras y en la unidad con la ayuda de los sargentos operadores de VoIP se ha llegado a la siguiente conclusión en relación con la gestión de estas:

La gestión de la centralita de Asterisk es más intuitiva. Su display es más amigable y ayuda a ello. La selección de pestañas es un método de configuración más rápido que ir metiendo comandos e ir levantando interfaces uno por uno como se hace con la centralita de Cisco. Debido a la mayor experiencia de los suboficiales con los sistemas de Cisco hace que esa velocidad con la pantalla web de Asterisk quede reducida. Debido a lo anteriormente expuesto, ambas centrales están en igualdad en tiempo requerido para su gestión [ver Anexo V].



6.4 SERVICIOS Y COMPATIBILIDADES

Este subcapítulo se enfoca en el análisis de qué central tiene mejores compatibilidades a la hora de enganchar terminales finales, y su interconexión con otros nodos.

La central Asterisk tolera mejor el reconocimiento de teléfonos de distintas marcas, cosa que a Cisco le cuesta más. Pero no es imposible, porque la central estudiada aceptaría otros teléfonos si se le instala los firmwares de algunas marcas. Aunque esto conlleva más tiempo. Por no hablar que los teléfonos de Cisco son Plug and Play, ósea, enchufar y a funcionar. Empate entre ambas centrales.

6.5 PRESUPUESTO

Este subcapítulo se analizará el presupuesto donde se observa que el sistema de Asterisk es el más económico de adquirir. La eficiencia en el consumo de recursos es importante en el Ministerio de Defensa, y en el que la opinión pública y los medios de comunicación son más críticos a la hora de justificar el gasto. Asterisk sería la más apropiada.

6.6 ELECCIÓN DE CENTRAL

En este subcapítulo se concluye que elección es elegida después del análisis de los apartados anteriores. Con un resultado en el que Cisco destaca en dos apartados con respecto a uno en el que destaca Asterisk habiendo igualdad en otros dos apartados, la central elegida sería la de Cisco. A parte que, en las entrevistas realizadas con los operadores encargados de su gestión, se decantaron a favor del sistema de Cisco [ver Anexo IV].

7 CONCLUSIONES

Dentro de este capítulo se van a exponer las conclusiones y las líneas futuras obtenidas del Trabajo de Fin de Grado, las cuales han sido extraídas de la realización de la investigación, así como de cada una de las pruebas realizadas en las EPCIS y en la unidad.

Como resultado de estos trabajos se puede ver en los siguientes puntos diferentes valoraciones:

- Se ha hecho evidente la importancia de la VoIP en el Ejército de Tierra, ejemplo de ello es la creación de secciones propias para la VoIP en la BRIPAC, debido a la imperiosa necesidad de actualización de los equipos que antes formaban la RBA.
- La importancia del ancho de banda en las transmisiones militares es un factor presente en el día a día en el campo, cosa que mejoraría mucho con estos gestores de llamadas por su optimización del tráfico IP
- La escalabilidad que permiten estas centrales telefónicas analizadas, situación que no permiten los CM integrados que van en los terminas ATQH y TLB50-IP actualmente en dotación en el ET, es esperanzador a la hora de gestionar una maniobra siendo la Brigada independiente de organismos superiores. Haciendo a esta una unidad más autónoma y



operativa.

- La seguridad que proporciona un CM debido al avance tecnológico nada tiene que ver con los años anteriores. No se está diciendo de abandonar los cifradores. Pero en los casos de unidades expedicionarias como la BRIPAC permite cumplir con esa dualidad operatividad-seguridad que mi tutor militar el Capitán Jefe de la CIATRANSPAC tanto hincapié hizo en nuestras entrevistas.
- La elección de una de estas centrales es vital para la mejora de las transmisiones en general. Por la unificación de servicios, su eficacia y ahorro de costes y equipos a largo plazo.
- La gestión es sin duda el punto más importante para los Suboficiales operadores de la Compañía de Transmisiones de la BRIPAC en concreto y de las Brigadas en general. Su consejo y opinión se han tenido muy en cuenta en este apartado, pues son los que levantan los terminales y se encargan de su configuración, siendo los mayores expertos en esta materia como las centralitas de los terminales satélite ATQH y TLB50-IP no pueden ser configuradas por la unidad, es necesario la implantación de estas centrales propias de la Compañía.
- La compatibilidad deber ser total y absoluta entre todos los equipos disponibles en dotación. Aunque el sistema de código abierto de Asterisk es a priori la opción más factible, los sistemas de Cisco están plenamente integrados en las unidades ya que se llevan más años de cooperación. Por no hablar que los contratos de confidencialidad firmados entre el Ministerio y la empresa hacen que esta deba cumplir unos estándares de compatibilidad y seguridad que, en caso de no ser cumplidos, Cisco se vería involucrada en posibles multas y la rescisión de contratos futuros. Aun con todo, ambas soluciones son aceptables, teniendo que adaptarse a los presupuestos disponibles.

7.1 LINEAS FUTURAS

Las Líneas futuras del TFG van orientadas al estudio de mejora de la VoIP. Encaminadas a mejorar el sistema de telecomunicaciones militares puesto en marcha ya hace algunos años con unidades más desarrolladas que otras. Las líneas futuras de investigación podrían ser las siguientes:

1. La homogeneización de toda la VoIP del Ejército. Teniendo todas las unidades una capacidad de conocimiento y desarrollo similar. Es decir, el uso que se de estas centrales este en el mismo nivel. Es cierto que cada unidad tendrá una arquitectura mayor o menor. Pero que en cada ejercicio se haga uso de estos medios para así mejorar la interoperabilidad entre unidades. Su conexión, en definitiva.
2. La actualización de los medios disponibles en las brigadas. Unificando en todas ellas los modelos disponibles, y haciéndolas interoperables con los Regimientos de Transmisiones. La adquisición de terminales compatibles con las centrales para su uso y optimización de medios.
3. Utilizar líneas terrenas, como el CECOM (Centro de Comunicaciones de las Unidades), introduciendo la telefonía IP de nuestro CM en las líneas RCT.
4. Usar los teléfonos terminales que permiten las videollamadas, ósea la integración



de la voz con el video.

5. Usar el servicio de línea directa (llamada en caliente) que permite el CM sin necesidad de marcación previa. Una especie de sistema de atención al usuario que dirija las llamadas automáticamente a un departamento o usuario determinado incluyendo traducción de voz a texto.

8 REFERENCIAS BIBLIOGRÁFICAS

[1] Matango, F. (2016). "Estado del Arte (VoIP)". *Server VoIP*. Disponible en: <http://www.servervoip.com/blog/estado-del-arte-voip/> [Consultado: 26-09-2022].

[2] Unión Internacional de Telecomunicaciones (2022). "EL FUTURO DE LA VOZ – SITUACIÓN DE LA VoIP". Disponible en: <https://www.itu.int/itu-news/manager/display.asp?lang=es&year=2007&issue=02&ipage=futureVoice2&ext=html> [Consultado: 26-09-2022].

[3] Carter, R. (2022). "La lista definitiva de estadísticas de VoIP (2022)". *Findstack*. Disponible en: <https://findstack.com/es/voip-statistics/> [Consultado: 26-09-2022].

[4] ¿Qué son Comunicaciones Unificadas? (2022). Zaragoza: 3CX. Disponible: <https://www.3cx.es/voip-sip/comunicaciones-unificadas/> Consultado: (27-09-2022)

[5] Gil, D. (2020). "7 ventajas de la VoIP frente a la telefonía tradicional". *Sarenat*. Disponible en: <https://blog.sarenat.es/ventajas-voip-telefonía-analógica/> [Consultado: 27-09-2022].

[6] Fernando Mendioroz, MSc. (2014). Sistemas de Conmutación, Señalización en Redes Telefónicas. Trabajo Fin de Grado. Universidad del Cauca. Disponible: <https://es.slideshare.net/fernandomendioroz/señalización-en-redes-telefónicas-pblicas-conmutadas-ss7-dss1-sigtran> [Consultado: 30-09-2022]

[7] Mantango, F. (2016). Protocolo de VoIP H.323. *Server VoIP*. Disponible: <http://www.servervoip.com/blog/protocolo-de-voip-h-323/> [Consultado: 1-10-2022]

[8] Protocolo de iniciación de sesión. (2022). En: Wikipedia, la enciclopedia libre. 4 de octubre Disponible en: https://es.wikipedia.org/wiki/Protocolo_de_iniciación_de_sesión [Consultado 11-10-2022]

[9] ¿Qué son métodos / solicitudes y respuestas SIP? (2022). 3CX. Disponible: <https://www.3cx.es/voip-sip/sip-methods/> [Consultado: 1-10-2022]

[10] SIP (2022). *3cuellectronica*. Disponible: <https://sites.google.com/site/3cuellectronica/home/voip/sip?tmpl=%2Fsystem%2Fapp%2Ftemplates%2Fprint%2F&showPrintDialog=1> [Consultado: 2-10-2022]

[11] Skinny Client Control Protocol (2019). En: Wikipedia, la enciclopedia libre. 1 de agosto. Disponible en: https://es.wikipedia.org/wiki/Skinny_Client_Control_Protocol [Consultado 11-10-2022]



[12] Media Gateway Control Protocol (2020). En: Wikipedia, la enciclopedia libre. 30 de marzo. Disponible en: https://es.wikipedia.org/wiki/Media_Gateway_Control_Protocol [Consultado 11-10-2022]

[13] QUE ES LA LATENCIA Y CÓMO AFECTA A LA VOZ IP. 2022. *Gesditel*. Disponible: <https://gesditel.es/que-es-la-latencia/> [Consultado: 14-10-2022]

[14] Jitter (2022). En: Wikipedia, la enciclopedia libre. 29 de mayo. Disponible en: <https://es.wikipedia.org/wiki/Jitter> [Consultado 14-10-2022]

[15] Mantango, F. (2016) Calidad de servicio de transmisión de voz con el protocolo Internet (VoIP). *Server VoIP*. Disponible: <http://www.servervoip.com/blog/tag/perdida-de-un-paquetes/#:~:text=Existen%20cuatro%20causas%20posibles%20para%20la%20p%C3%A9rdida%20de%20paquetes%3A&text=Retardo%20en%20el%20extremo%20receptor,fase%20de%20la%20memoria%20tamp%C3%B3n%3B&text=Destrucci%C3%B3n%20por%20un%20m%C3%B3dulo%20congestionado%3B&text=Paquete%20no%20v%C3%A1lido%20debido%20a%20fallos%20de%20transmisi%C3%B3n>. Consultado: [14-10-2022]

[16] VOIP AUDIO CODECS. (2022) *Sip System Blog*. Disponible: <https://sip-systems.com/f/voip-audio-codecs/> [Consultado: 14-10-2022]

[17] Conversion de la señal analógica en digital. (2022). *Ikastaroak*. Disponible: https://ikastaroak.ulhi.net/edu/es/IEA/ICTV/ICTV02/es_IEA ICTV02 Contenidos/website_522_conversion_de_la_seal_analgica_en_digital.html [Consultado: 18-10-2022]

ANEXOS

Anexo I:

Funcionamiento protocolo SIP

En este anexo se detalla el proceso elemental de comunicación interna de una centralita IP usando el protocolo SIP.

- Diferencia entre el establecimiento y la



descripción de la sesión

- Extensible
- Protocolo de extremo a extremo
- Un usuario ES DUEÑO DE SU SESIÓN
- Paradigma IP vs. Paradigma SS7
- Favorece la interoperabilidad
- El 'core' es "relativamente" sencillo: 6

métodos

- Funcionalidades adicionales mediante extensiones
- Es escalable
- La inteligencia está en los extremos
- La red guarda muy pocos datos del estado
- INVITE
- Invita a un usuario a una sesión multimedia
- Modifica una sesión multimedia existente
- ACK
- Proporciona un 3-way-handshake en el INVITE, sirve para confirmar la recepción de una respuesta final a un INVITE
- CANCEL
- Cancela una transacción en curso
- BYE
- Se utilizan para abandonar una sesión
- REGISTER
- Sirven para informar al servidor de la ubicación del usuario
- OPTIONS
- Nos permite consultar qué métodos soporta un usuario.
- Un cliente GENERA peticiones.
- Un servidor RECIBE peticiones.
- El UA que genera peticiones se conoce como UAC: User Agent Client.
- El UA que responde a las peticiones se conoce como UAS: User Agent Server.



- Una petición, junto con las respuestas que genera, es una TRANSACCIÓN.
- 100 – 199: provisional e informativa
- 200 – 299: afirmativa
- 300 – 399: redirección
- 400 – 499: error del cliente
- 500 – 599: error del servidor
- 600 – 699: fallo global
- Las respuestas incluyen un mensaje descriptivo, pero lo importante es el código numérico.

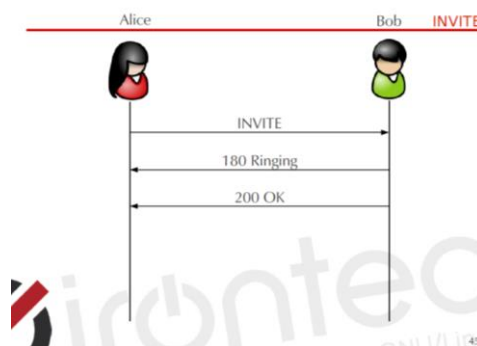


Ilustración 1. Invite. Fuente: Irontec.com

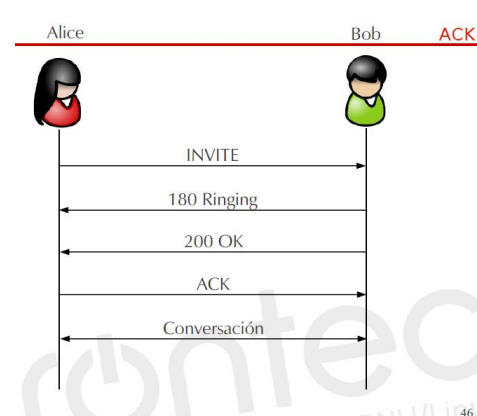


Ilustración 2. ACK. Fuente: Irontec.com

- INVITE es el único método que utiliza 3 way handshake.
- El resto de los mensajes esperan una respuesta veloz, pero en el caso del INVITE, esta puede tardar.



- El UAC manda al UAS un ACK, indicando que ha recibido su respuesta.
- Aseguramos el correcto establecimiento de la sesión sobre un medio no fiable: UDP

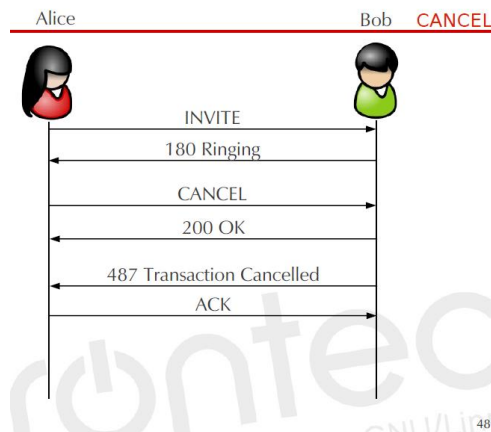


Ilustración 3. Cancel. Fuente: Irontec.com

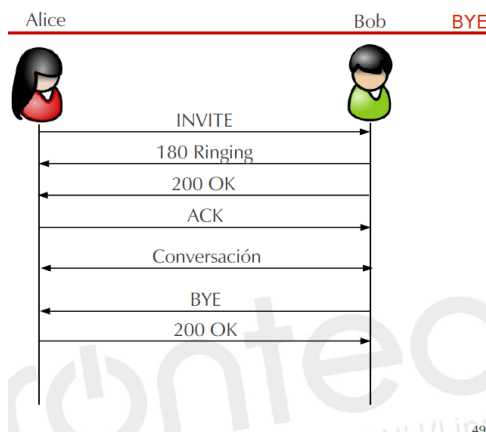


Ilustración 4. Bye. Fuente: Irontec.com

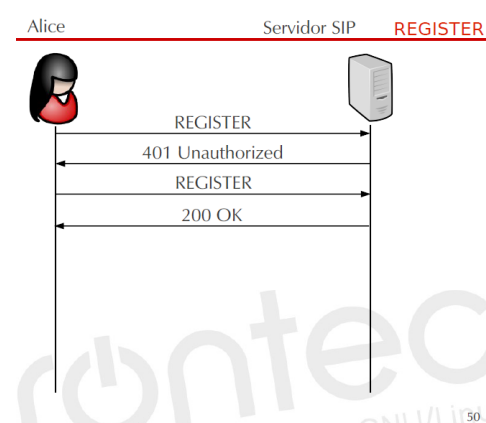


Ilustración 5. Register. Fuente: Irontec.com

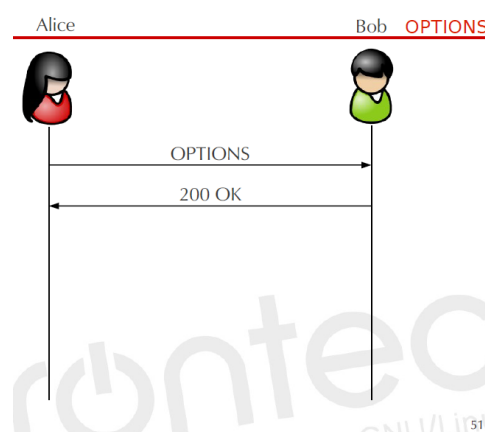


Ilustración 6. Options. Fuente: Irontec.com

Anexo II:

Asterisk como PBX “normal”

En estas ilustraciones se aprecia un esquema simple de la conexión de una PBX Asterisk en diferentes casos. Con una centralita de Cisco se podría realizar el mismo conexionado. Se aporta este anexo para su sencilla comprensión esquemática.

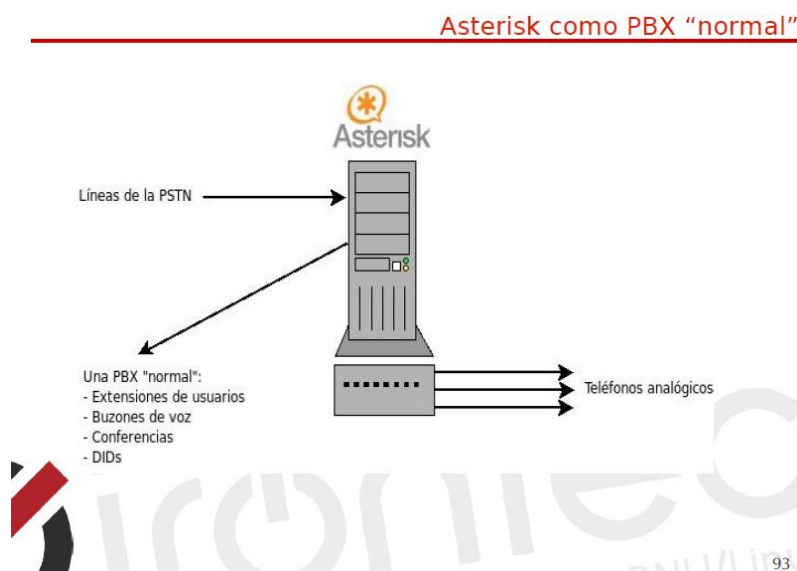


Ilustración 7. PBX Asterisk. Fuente: Irontec.com



Una PBX VoIP

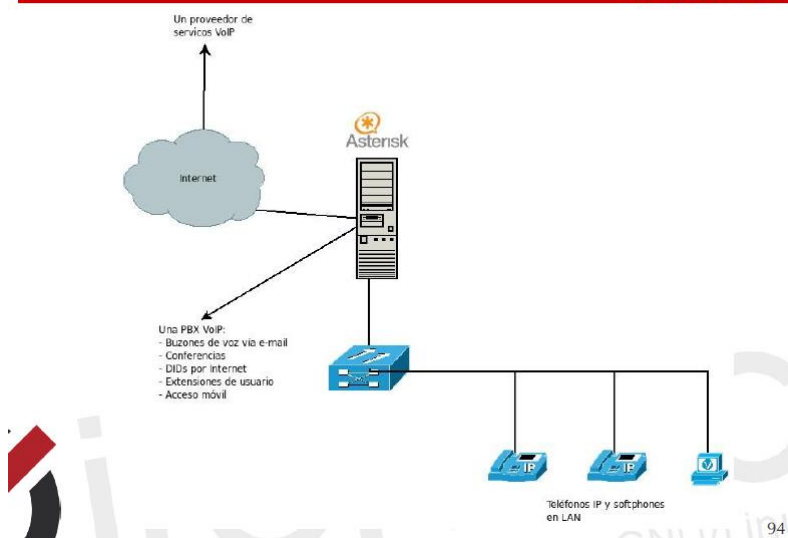


Ilustración 8. VoIP con PBX. Fuente: Irontec.com

Complemento/ampliación de una PBX tradicional

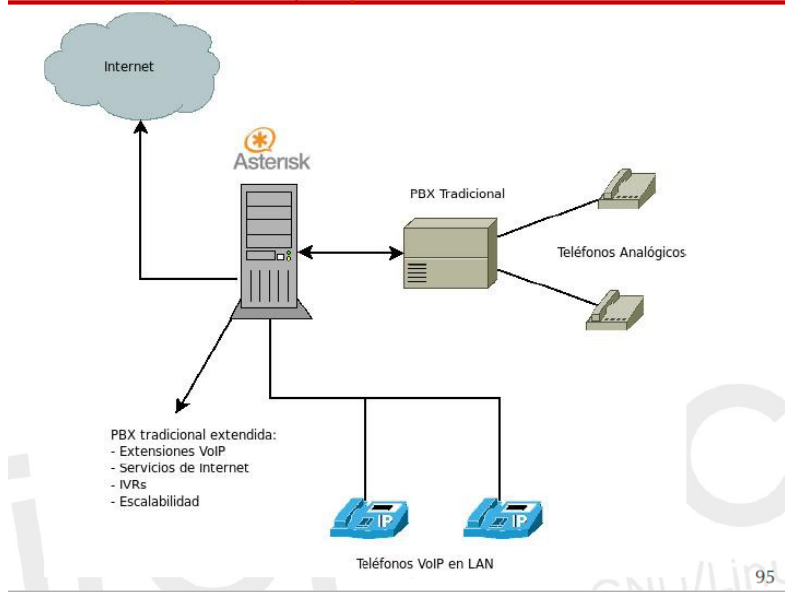


Ilustración 9. PBX más PBX analógica. Fuente: Irontec.com



Gateway VoIP - PSTN

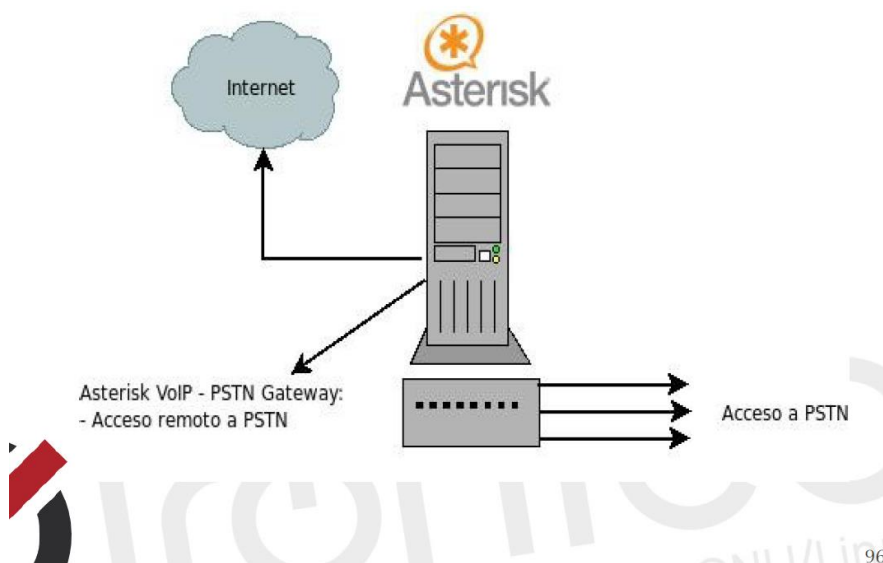


Ilustración 10. PBX con pasarela a red analógica. Fuente: Irontec.com

Anexo III:

Configuración básica de un CME de Cisco con sus teléfonos y diversos servicios.

Este anexo contiene el proceso y los comandos a utilizar en la administración de un Call Manager de Cisco y como registrar sus teléfonos y añadirle funciones como buzón de voz.

• Introducción

Este documento proporciona una configuración de muestra para Cisco CallManager Express (CME) 4.0 y Cisco Unity Express (CUE) 2.2.2 e información sobre cómo integrar estos dos sistemas en su red de telefonía.

• Prerequisites

• Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Instale el hardware apropiado.
- Descargue e instale el software de Cisco IOS® apropiado.
- Descargue el software de Cisco Unified CallManager Express.



- Descargue el software de Cisco Unity Express.

• **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco 3725 con software Cisco IOS versión 12.4(9)T
- Switch Cisco Catalyst 3550 con software Cisco IOS versión 12.1
- Teléfono IP 7960 de Cisco
- Cisco Unified CallManager Express 4.0
- Cisco Unity Express 2.2.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

• **Configurar**

En esta sección se ofrece información para configurar las funciones descritas en este documento.

• **Diagrama de la red**

En este documento, se utiliza esta configuración de red:

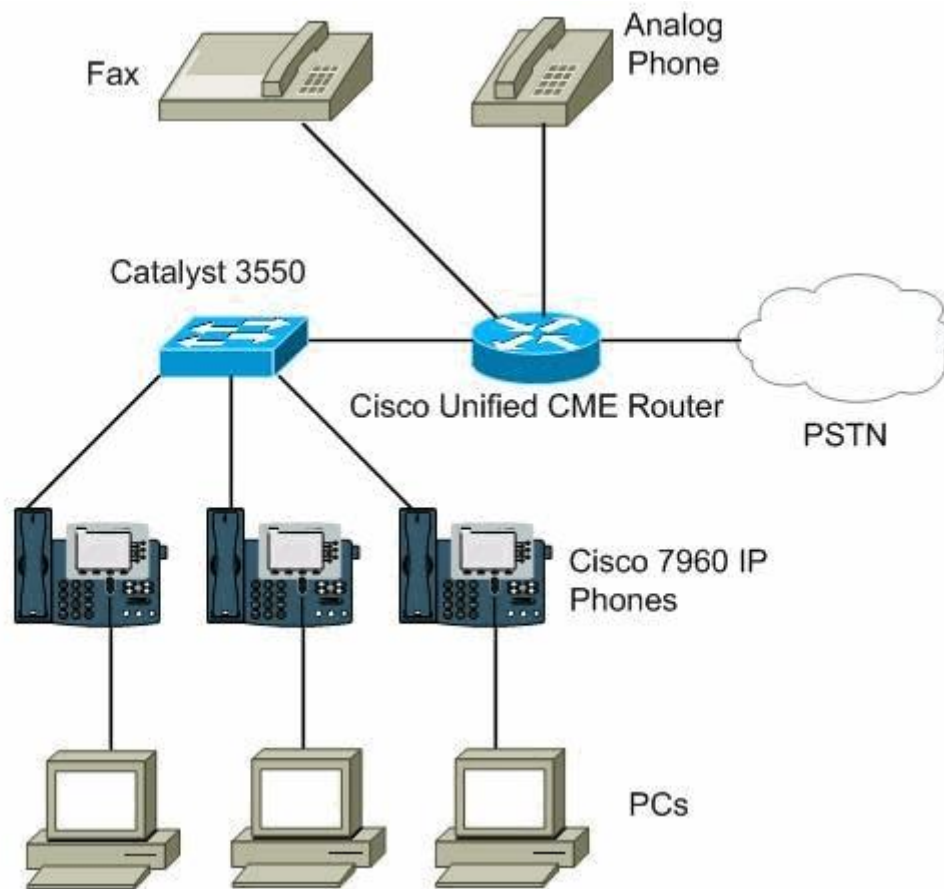


Ilustración 11. Esquema de red. Fuente: Cisco

- **Definir un servidor DHCP local**

En una red de telefonía IP optimizada, las direcciones IP de los teléfonos y los PC se deben configurar en diversos segmentos de red. El protocolo de configuración dinámica de host (DHCP) permite asignar automáticamente las direcciones IP reutilizables a los clientes DHCP. La característica del servidor DHCP de Cisco IOS es la implementación completa del servidor DHCP que asigna y administra las direcciones IP de los grupos de direcciones especificados en el router a los clientes DHCP. Si el servidor DHCP de Cisco IOS no cumple con la solicitud DHCP de la base de datos, puede reenviar la solicitud a uno o más servidores DHCP secundarios definidos por el administrador de la red.

La Figura 1 muestra los pasos básicos que ocurren cuando un cliente DHCP solicita una dirección IP de un servidor DHCP. El cliente (host A) envía el mensaje de difusión DHCPDISCOVER para localizar un servidor DHCP de Cisco IOS. El servidor DHCP ofrece los parámetros de configuración, como dirección IP, dirección MAC, nombre de dominio y asignación para la dirección IP, al cliente a través del mensaje de unidifusión DHSCPOFFER.



Solicitud DHCP para una dirección IP desde un servidor DHCP

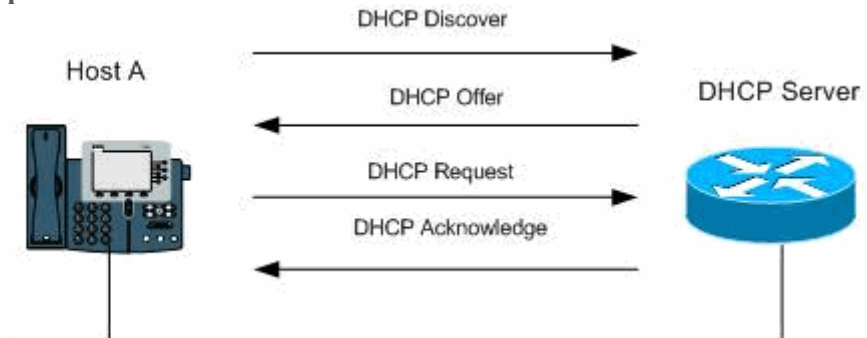


Ilustración 12. Solicitud DHCP. Fuente: Cisco

El cliente devuelve una solicitud formal para la dirección IP ofertada al servidor DHCP en un mensaje de broadcast DHCPREQUEST. El servidor DHCP confirma que la dirección IP está asignada al cliente con la devolución del mensaje de unidifusión DHCPACK al cliente.

Para esta configuración, debe crear dos servidores DHCP locales; uno para voz y otro para datos. Cuando cree los dos servidores DHCP, tendrá dos subredes diferentes que facilitarán el proceso de asignación de las direcciones correctas sin ningún conflicto.

Este procedimiento crea un grupo compartido de direcciones IP donde todos los clientes DHCP reciben la misma información, que incluye la opción 150 (dirección IP del servidor TFTP). La ventaja de elegir este método para configurar el servicio DHCP es que solo se configura un conjunto DHCP.

1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración global.
4. Router#**configure terminal**
5. Introduzca el comando **ip dhcp pool pool-name** para crear un nombre para el conjunto de direcciones del servidor DHCP e ingresar en el modo de configuración del conjunto DHCP.
6. Router(config)#**ip dhcp pool Voice**
7. Introduzca el comando **network ip-address mask** para especificar la dirección IP del conjunto de direcciones DHCP y la máscara opcional.
8. Router(dhcp-config)#**network 172.22.100.0 255.255.255.0**
9. Introduzca el comando **option 150 ip ip-address** para especificar la dirección del servidor TFTP desde la cual el teléfono IP de Cisco Unified descarga el archivo de configuración de la imagen.
10. Router(dhcp-config)#**option 150 ip 172.22.1.107**



11. Introduzca el comando **default-router ip-address** para especificar el router que los teléfonos IP utilizan para enviar o recibir tráfico IP que es externo a su subred local.
12. Router (dhcp-config) #**default-router 172.22.100.1**
13. Introduzca el comando **end** para finalizar la configuración.
14. Router (dhcp-config) #**end**

Nota: Repita el mismo procedimiento para crear un servidor DHCP local para el rango de direcciones de datos.

• Configurar las interfaces del router

En este caso, la plataforma 3725 contiene dos interfaces FastEthernet que pueden utilizarse para conectarse con el switch de núcleo. Sin embargo, deseará poder usar solo una interfaz para transmitir el tráfico de datos, el tráfico de voz y tener acceso a Internet a través del gateway predeterminado. Un buen método que permite esto es la comunicación interVLAN, donde el router tiene la capacidad de dividir una de sus interfaces en varias subinterfaces para crear diversos segmentos lógicos o VLAN. Con esta función, el router puede recibir paquetes en una VLAN y reenviarlos a otra VLAN. Deberá habilitar Inter Switch Link (ISL) o enlaces troncales 802.1Q en una misma conexión física entre el switch y el router para lograr esto. Una vez configuradas las direcciones IP en las subinterfaces, el router reconoce la red asociada con cada VLAN como una red directamente conectada.

La Figura 2 muestra un router conectado a un switch con la interfaz FastEthernet 0/0 conectada a un puerto de enlace troncal en un switch. La interfaz FastEthernet se divide en un interfaceador lógico, subinterfaces para cada VLAN y una dirección IP para actuar como gateway para cada dominio de difusión.

Configuración del routing interVLAN

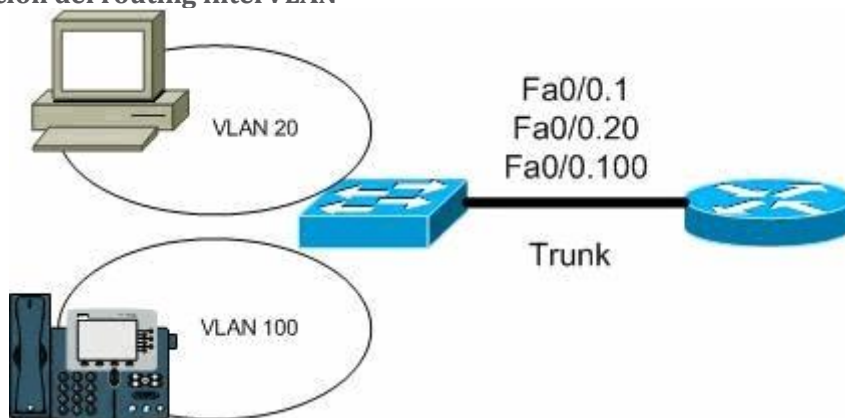


Ilustración 13. Separación por Vlanes. Fuente: Cisco



Esto muestra la configuración requerida para el router 3725 que utiliza la etiqueta de tramas 802.1Q:

1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración global.
4. Router#**configuration terminal**
5. Introduzca el comando **interface fastethernet port** para ingresar al modo de configuración de la interfaz.
6. Router(config)#**interface fastethernet 0/0.1**
7. Introduzca el comando **encapsulation [dot1q/ISL] id-num native** para crear la VLAN nativa.
8. Router(config-if)#**encapsulation dot1q 1 native**
9. Introduzca el comando **ip address ip-address mask** para asignar una dirección válida a la interfaz.
10. Router(config-if)#**ip address 172.22.1.154 255.255.255.0**
11. Introduzca el comando **exit** para salir de la configuración de esa interfaz.
12. Router(config-if)#**exit**
13. Introduzca el comando **interface fastethernet port.id-num** para crear e ingresar la configuración de la subinterfaz de voz.
14. Router(config)#**interface fastethernet 0/0.100**
15. Introduzca el comando **encapsulation [dot1q/ISL] id-num** para habilitar el tronco.
16. Router(config-if)#**encapsulation dot1q 100**
17. Introduzca el comando **ip address ip-address mask** para asignar una dirección válida a la subinterfaz de voz.
18. Router(config-if)#**ip address 172.22.100.1 255.255.255.0**
19. Introduzca el comando **interface fastethernet port.id-num** para crear e ingresar la configuración de su subinterfaz de datos.
20. Router(config)#**interface fastethernet 0/0.20**
21. Introduzca el comando **encapsulation [dot1q/ISL] id-num** para habilitar el tronco.
22. Router(config-if)#**encapsulation dot1q 20**
23. Introduzca el comando **ip address ip-address mask** para asignar una dirección válida a la subinterfaz de datos.
24. Router(config-if)#**ip address 172.22.101.1 255.255.255.0**
25. Introduzca el comando **end** para finalizar la configuración.
26. Router(config-if)#**end**

- **Establecer el protocolo de tiempo de red**

El protocolo de tiempo de red (NTP) le permite sincronizar su router de Cisco Unified CallManager Express con un único reloj en la red, denominado reloj maestro. El NTP está



deshabilitado en todas las interfaces de forma predeterminada, pero es esencial para Cisco Unified CallManager Express. Por lo tanto, debe asegurarse de que esté habilitado. Este procedimiento muestra los pasos para habilitar el NTP en Cisco 3725:

1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración global.
4. Router#**configure terminal**
5. Introduzca el comando **clock timezone zone hours-offset** para establecer la zona horaria local.
6. Router(config)#**clock timezone central -8**
7. Introduzca el comando **clock summer-time zone recurring** para especificar el horario de verano. Como valor predeterminado, el horario de verano está deshabilitado.
8. Router(config)#**clock summer-time central recurring**
9. Introduzca el comando **ntp server ip-address** para permitir que el reloj de este router se sincronice con el servidor NTP especificado. En este caso, es la misma dirección que la del servidor TFTP.
10. Router(config)#**ntp server 172.22.1.107**
11. Introduzca el comando **end** para finalizar la configuración.
12. Router(config)#**end**

- **Configurar las VLAN en un switch Catalyst 3550**

Puede crear diversas redes de área local virtuales (VLAN) para separar el tráfico existente en una VLAN de las demás y así aislar el tráfico de voz del de datos. Cree dos VLAN, una para voz y otra para datos, en un switch Catalyst para lograrlo. Con esto, creará dos subredes lógicas que crean múltiples dominios de difusión y previenen la posibilidad de bucles en la red. De hecho, los teléfonos y las PC están conectados físicamente, pero separados lógicamente en diversas subredes. Estos son los pasos para crear una VLAN para voz en un switch Catalyst 3550.

La Figura 3 muestra cómo las VLAN permiten que el switch tenga múltiples dominios de difusión en un entorno con switches. Se crean una VLAN para voz y una VLAN para datos. Dos subredes completamente separadas permiten que los teléfonos y las PC se comuniquen a través de las VLAN correspondientes.



Descripción general de la VLAN

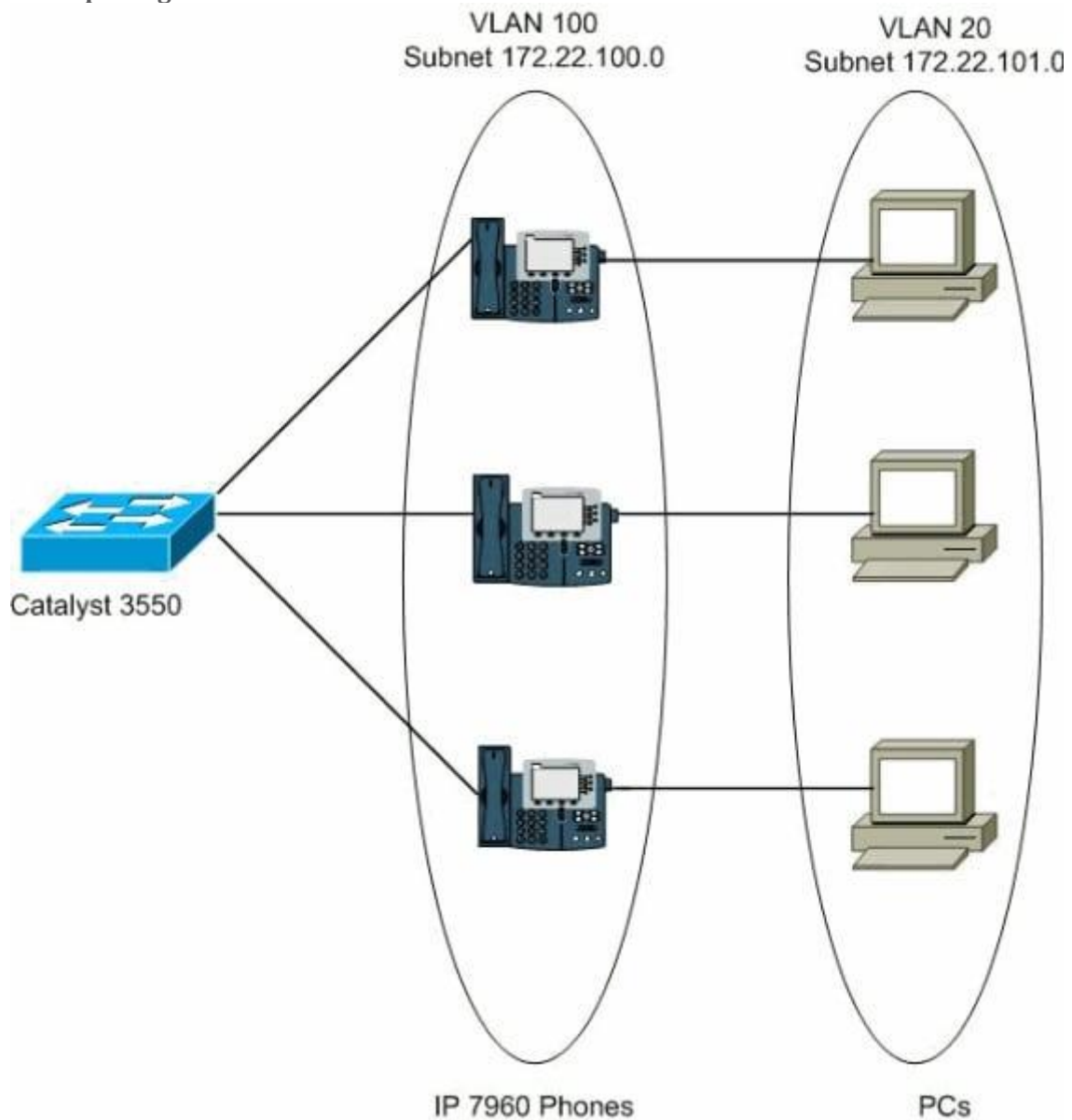


Ilustración 14. Conexión de ordenador a través de teléfono IP. Fuente: Cisco

1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. Switch>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración global.
4. Switch#**configure terminal**
5. Introduzca el comando **vlan vlan-id** para crear una VLAN en el switch.
6. Switch(config) #**vlan 100**
7. Introduzca el comando **name vlan-name** para dar un nombre a la VLAN.
8. Switch(config) #**name Voice**
9. Introduzca el comando **end** para finalizar la configuración.
10. Switch(config) #**end**



Nota: Repita el mismo procedimiento para crear una VLAN para datos.

- **Configurar una interfaz en un switch Catalyst 3550**

Deberá configurar la interfaz que se conecta con el router para completar el proceso de enlace troncal entre el router Cisco 3725 y el switch Catalyst 3550. La configuración en la interfaz del switch debe ser la misma que la configuración en la interfaz del router, de modo que el enlace troncal pueda llevar el tráfico de diversas VLAN a través de un único enlace. Puede crearse una interfaz de VLAN, por ejemplo, int vlan 1, para cada VLAN configurada en el switch. En este caso, utilice la VLAN de la interfaz predeterminada (int vlan 1) para VLAN de administración. Una vez creada y configurada correctamente la VLAN de la interfaz, deberá habilitar enlaces troncales en la interfaz. Esta es la configuración para la interfaz del switch Catalyst 3550:

1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. Switch>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración global.
4. Switch#**configure terminal**
5. Introduzca el comando **interface vlan vlan-id** para ingresar a la interfaz que desea configurar.
6. Switch(config)#**interface vlan 1**
7. Introduzca el comando **ip address ip-address mask** para dar a la interfaz una dirección válida
8. Switch(config-if)#**ip address 172.22.1.201 255.255.255.0**
9. Introduzca el comando **exit** para finalizar la configuración de esa interfaz.
10. Switch(config-if)#**exit**
11. Introduzca el comando **ip default-gateway ip-address** para dar acceso a la red externa.
12. Switch(config)#**ip default-gateway 172.22.1.1**
13. Introduzca el comando **interface fastethernet port** para ingresar a la interfaz que debe habilitarse para el trunking
14. Switch(config)#**interface fastethernet 0/19**
15. Introduzca el comando **switchport trunk encapsulation [dot1q/ISL]** para elegir el método en el que se etiquetan las tramas.
16. Switch(config-if)#**switchport trunk encapsulation dot1q**
17. Introduzca el comando **switchport mode trunk** para habilitar el tronco.
18. Switch(config-if)#**switchport mode trunk**
19. Introduzca el comando **switchport trunk allowed vlan all** para permitir todas las VLAN en el trunk.
20. Switch(config-if)#**switchport trunk allowed vlan all**



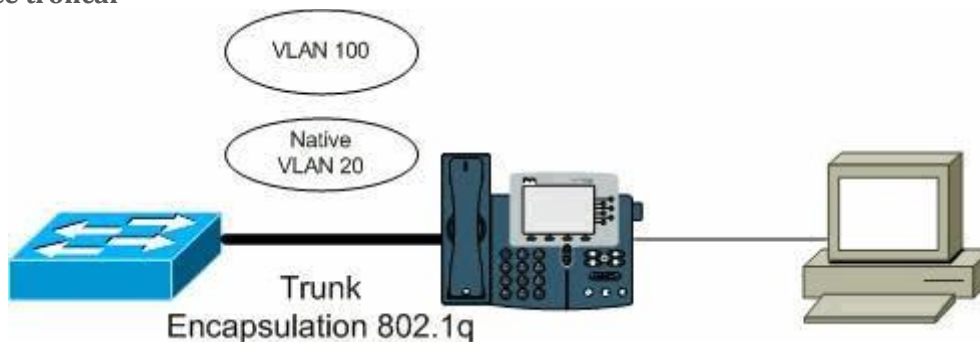
21. Introduzca el comando **duplex [full/half]** para habilitar el modo dúplex, igual que el dúplex de ese router.
22. `Switch(config-if) #duplex full`
23. Introduzca el comando **speed number** para establecer la velocidad de los datos.
24. `Switch(config-if) #speed 100`
25. Introduzca el comando **end** para finalizar la configuración.
26. `Switch(config-if) #end`

• Configurar el puerto para conectar a un teléfono IP Cisco 7960

El teléfono IP Cisco 7960 admite la conexión a una PC u otro dispositivo. Por este motivo, la interfaz que conecta la familia de switches Catalyst 3550 con el teléfono IP Cisco 7960 puede llevar una mezcla de tráfico de datos y voz. Deberá configurar la interfaz como enlace troncal para poder llevar el tráfico de las VLAN de datos y voz a través de un único enlace y permitir que se extiendan por toda la red. Una vez habilitado el modo troncal, se deben configurar los dos puertos de switch para las diversas VLAN a fin de especificar cómo se dividirá el tráfico. Configure una VLAN de voz para llevar el tráfico de voz y una VLAN nativa para permitir que el resto del tráfico viaje sin etiquetas por esta VLAN. Realice este procedimiento para configurar un puerto para llevar el tráfico de voz y datos en las diversas VLAN.

La Figura 4 muestra un enlace troncal creado entre el switch y el teléfono. El enlace troncal refleja un tipo 802.1q de encapsulamiento y las diversas VLAN a las que se les permite extenderse por la red.

Enlace troncal



1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. `Switch>enable`
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración global.
4. `Switch#configure terminal`
5. Introduzca el comando **interface fastethernet port** para ingresar el puerto utilizado para conectar el teléfono.
6. `Switch(config) #interface fastethernet0/21`



7. Introduzca el comando **switchport mode trunk** para configurar el puerto como troncal VLAN.
8. Switch(config-if) #**switchport mode trunk**
9. Introduzca el comando **switchport trunk encapsulation dot1q** para configurar el puerto para soportar la encapsulación 802.1q.
10. Switch(config-if) #**switchport trunk encapsulation dot1q**
11. Introduzca el comando **switchport voice vlan vlan-id** para indicar al teléfono IP de Cisco que reenvíe todo el tráfico de voz a través de la VLAN especificada.
12. Switch(config-if) #**switchport voice vlan 100**
13. Introduzca el comando **switchport trunk native vlan vlan-id** para indicar al teléfono IP de Cisco que reenvíe todo el tráfico de datos a través de la VLAN especificada.
14. Switch(config-if) #**switchport trunk native vlan 20**
15. Introduzca el comando **end** para finalizar la configuración.
16. Switch(config-if) #**end**

• Configurar los parámetros de Cisco Unified CallManager Express

El siguiente paso en el proceso de configuración modifica los archivos de configuración de lenguaje de marcado extensible (XML) del teléfono, de modo que los teléfonos IP puedan encontrar automáticamente los valores predeterminados para configurarlos cuando estén en línea o se reinicien. Por motivos de seguridad, desactive la opción de registro automático para evitar la conexión de cualquier teléfono sin permiso. Este procedimiento establece los valores para los parámetros de telefonía que el sistema Cisco Unified CallManager Express requiere. Con este procedimiento, usted genera los archivos de configuración. Por lo tanto, los teléfonos pueden descargar los valores de parámetros para restablecerse a sí mismos.

1. Introduzca el comando **enable** para ingresar al modo EXEC privilegiado.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **tftp-server flash:filename** para permitir que el router Cisco CallManager Express proporcione acceso TFTP al archivo especificado por el teléfono IP atendido por el router.
6. Router(config) #**tftp-server flash:P00307020300.bin**
7. Introduzca el comando **telephony-service** para ingresar al modo de configuración telefónica.
8. Router(config) #**telephony-service**
9. Introduzca el comando **max-ephones max-num-phones** para establecer el número máximo de teléfonos IP que admite esta plataforma.
10. Router(config-telephony) #**max-ephones 144**



11. Introduzca el comando **max-dn max-directory-numbers** para establecer el número máximo de extensiones que pueden existir en esta plataforma.
12. Router (config-telephony) #**max-dn 500**
13. Introduzca el comando **no auto-reg-ephone** para evitar la conexión de cualquier teléfono al sistema.
14. Router (config-telephony) #**no auto-reg-ephone**
15. Introduzca el comando **load phone-type firmware-file** para identificar el archivo de firmware que el teléfono IP utiliza para registrarse en el sistema.
16. Router (config-telephony) #**load 7960 P0030700300**
17. Introduzca el comando **ip source-address ip-address** para identificar la dirección IP y el número de puerto que el router Cisco CallManager Express utiliza para el registro del teléfono IP. El puerto predeterminado es 2000.
18. Router (config-telephony) #**ip source-address 172.22.1.107**
19. Introduzca el comando **create cnf-files** para generar los archivos de configuración XML.
20. Router (config-telephony) #**create cnf-files**
21. Introduzca el comando **transfer-system full-consultant** para especificar el método de transferencia de llamada. Este es el método predeterminado.
22. Router (config-telephony) #**transfer-system full-consultant**
23. Introduzca el comando **secondary-dialtone 9** para crear otro tono cuando marque 9 para realizar una llamada externa.
24. Router (config-telephony) #**secondary-dialtone 9**
25. Introduzca el comando **end** para finalizar la configuración.
26. Router (config-telephony) #**end**

• Aprovechamiento de teléfonos IP

Los parámetros de Cisco Unified CallManager Express se establecen para que los teléfonos IP puedan registrarse y comenzar a funcionar. Sin embargo, antes de comenzar a hacer y recibir llamadas, debe registrar los teléfonos IP específicos que desea en el sistema de Cisco CallManager Express. En este proceso configurará los números de directorio de un teléfono Ethernet (ephone-dn) individual y asociará cada uno con uno o varios botones en uno o más teléfonos Ethernet (ephone). Cada ephone-dn es una línea virtual, o extensión, por donde pueden realizarse conexiones de llamadas. Cada teléfono físico debe configurarse como un ephone en el router de Cisco CallManager Express para recibir soporte en el entorno de la LAN. Con el uso de **ephone-dn** comando y palabra clave de línea dual que crea un ephone-dn en modo de línea dual. El motivo es contar con un puerto de voz y dos canales para manejar dos llamadas independientes. Este modo habilita las opciones de transferencia de llamadas, llamada en espera y conferencia. Este procedimiento registra los ephones y los ephones-dns con el modo de línea dual:

1. Introduzca el comando **enable** para ingresar al modo EXEC.



2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **ephone-dn dn-tag dual-line** para crear la extensión con dos canales.
6. Router(config)#**ephone-dn 11 dual-line**
7. Introduzca el comando **number number** para configurar un número de extensión válido.
8. Router(config-ephone-dn)#**number 1001**
9. Introduzca el comando **name name** para asociar un nombre a este ephone-dn.
10. Router(config-ephone-dn)#**name John Smith**
11. Introduzca el comando **exit** para salir de la configuración ephone-dn.
12. Router(config-ephone-dn)#**exit**
13. Introduzca el comando **ephone phone-tag** para ingresar la configuración física del teléfono.
14. Router(config)#**ephone 1**
15. Introduzca el comando **mac-address [mac-address]** para especificar qué teléfono está configurado.
16. Router(config-ephone)#**mac-address 0030.94C2.D6E7**
17. Introduzca el comando **type phone-type** para especificar el tipo de teléfono.
18. Router(config-ephone)#**type 7960**
19. Introduzca el comando **button button-number (separator) dn-tag** para asociar el número de botón y las características de línea con una extensión. En este caso, utilice un separador :(dos puntos) que implica un anillo normal.
20. Router(config-ephone)#**button 1:11**
21. Introduzca el comando **end** para finalizar la configuración.
22. Router(config-ephone)#**end**

- **Establecer un plan de marcado en Cisco CallManager Express**

El patrón de plan de marcado crea una secuencia de dígitos que especifica un prefijo global para la expansión de los números de extensión abreviados en números E.164 totalmente calificados. Con esta configuración, el sistema Cisco CallManager Express puede asociar un patrón de dígitos para un prefijo de número de extensión abreviado al patrón completo de número telefónico E.164. Este procedimiento muestra la configuración para el patrón de plan de marcado:

1. Introduzca el comando **enable** para ingresar al modo EXEC.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**



5. Introduzca el comando **telephony-service** para ingresar al modo de configuración del servicio de telefonía.
6. Router(config) #**telephony-service**
7. Introduzca el comando **dialplan-pattern tag pattern extension length length** para hacer coincidir el número de extensión con el teléfono.
8. Router(config-telephony) #**dialplan-pattern 1 5123781291 extension length 4**
9. Introduzca el comando **end** para finalizar la configuración.
10. Router(config-telephony) #**end**

• Conectar a la PSTN

Durante esta tarea, configure los puertos de voz FXO para admitir las conexiones a la red telefónica pública conmutada (PSTN). Configure el hardware (puertos de voz) y los pares de marcado requeridos para hacer y recibir llamadas entrantes y salientes a fin de conectar el teléfono hacia fuera de la red.

Esta configuración se divide en tres partes. En primer lugar, deberá configurar su puerto FXO para reenviar las llamadas entrantes a las extensiones que aceptan marcado, por ejemplo, una recepcionista que puede transferir la llamada entrante. Este procedimiento permite configurar los puertos FXO:

1. Introduzca el comando **enable** para ingresar al modo EXEC.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **voice-port slot/port** para ingresar al modo de configuración de puerto de voz y especificar qué puerto configurar. Este puerto es desde donde se conecta el cable del teléfono; en este caso, el puerto de voz 1/0.
6. Router(config) #**voice-port 2/1/0**
7. Introduzca el comando **connection plar digits** para especificar una conexión de línea privada, llamada automática (PLAR) y reenviar automáticamente la llamada entrante a la extensión especificada por el argumento digits.
8. Router(config-voiceport) #**connection plar 1001**
9. Introduzca el comando **caller-id enable** para permitir que se reciba la información del ID de la persona que llama en el puerto FXO configurado.
10. Router(config-voiceport) #**caller-id enable**
11. Introduzca el comando **exit** para salir de la configuración del puerto de voz.
12. Router(config-voiceport) #**exit**

En segundo lugar, deberá crear algunos pares de marcado para que el sistema Cisco CallManager Express asocie un número de teléfono a un puerto FXO en particular, de manera que puedan realizarse las llamadas salientes. Deberá crear tantos pares de marcado como necesite (llamadas locales, llamadas de larga distancia, llamadas



internacionales, etc.) teniendo en cuenta el diverso orden en que se manejarán y ciertas restricciones. Consulte para obtener más información sobre los pares de marcado. Deberá asignar un número de puerto de voz al par de marcado y un patrón de destinos. Este procedimiento configura el par de marcado para las llamadas locales:

1. Introduzca el comando **dial-peer voice tag pots** para configurar un par de marcado POTS saliente.
2. Router(config) **#dial-peer voice 1 pots**
3. Introduzca el comando **destination-pattern string** para especificar el patrón de los números que el usuario debe marcar para realizar una llamada que incluya números de prefijo y de destino.

Puede utilizar diversos caracteres para representar los números. Sin embargo, este procedimiento configura un par de marcado de llamada local con el prefijo 9 (marcado del número para realizar una llamada externa), [] (corchetes) para indicar un rango y seis "." (puntos) correspondientes a cada dígito ingresado.

```
Router(config-dial-peer) #destination-pattern 9[2-9].....
```

Nota: Los caracteres especiales ^ y \$ se cuentan como dígitos de correspondencia explícita; los patrones dentro de () no se cuentan como dígitos de correspondencia explícita.

4. Introduzca el comando **port slot/port** para especificar el puerto a través del cual se realizan las llamadas a este par.
5. Router(config-dial-peer) **#port 2/1/0**
6. Introduzca el comando **prefix number character-comma** para especificar que el número le da un tono de marcado para realizar una llamada externa.
7. Router(config-dial-peer) **#prefix 9,**
8. Introduzca el comando **end** para finalizar la configuración.
9. Router(config-dial-peer) **#end**

En tercer lugar, deberá crear un par de marcado para que el teléfono analógico pueda conectarse con un puerto Foreign Exchange Station (FXS). La interfaz FXS es un conector RJ-11 que permite la conexión del equipo telefónico básico, los teclados y la centralita privada (PBX), y ofrece tono de llamada, voltaje y tonos de marcado. Debe asignar el puerto de FXS a este par de marcado y darle un destino o una extensión para poder configurar los puertos FXS en el router. Este es el procedimiento para configurar los puertos FXS:

1. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
2. Router#**configure terminal**
3. Introduzca el comando **dial-peer voice tag pots** para configurar un par de marcado POTS saliente.
4. Router(config) **#dial-peer voice 5 pots**



5. Introduzca el comando **destination-pattern string** para especificar el patrón de los números que el usuario debe marcar para realizar una llamada. En este caso, asigne un patrón de destino con la misma longitud de extensión que los teléfonos IP, de modo que pueda evitar la confusión con el resto de los pares de marcado. Con el par de marcado, puede hacer llamadas locales, de larga distancia e internacionales desde un teléfono analógico.

```
Router(config-dial-peer) #destination-pattern 1005
```

6. Introduzca el comando **port slot/port** para especificar el puerto que corresponde a su interfaz FXS a través del cual se realizan las llamadas a este par.
7. Router(config-dial-peer) #**port 2/0/0**
8. Introduzca el comando **end** para finalizar la configuración.
9. Router(config-dial-peer) #**end**

• Activar la conectividad IP al software Cisco Unity Express

Ahora debe integrar Cisco Unity Express 2.2.2 con Cisco CallManager Express 4.0. Para ello, debe crear dos interfaces para que se lleve a cabo la comunicación entre Cisco Unity Express y Cisco Call Manager Express. La primera es una interfaz para el router que aloja Cisco CallManager Express, que ya se estableció anteriormente en la sección [Configurar las interfaces del router](#). La segunda es una interfaz que enlaza los puertos y las direcciones IP de Cisco Unity Express y Cisco CallManager Express. Complete estos pasos para realizar esta tarea:

1. Introduzca el comando **enable** para ingresar al modo EXEC.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **interface service-engine slot/unit** para ingresar al modo de configuración de la interfaz de Cisco Unity Express.
6. Router(config)#**interface service-engine 1/0**
7. Introduzca el comando **ip unnumbered type number** para especificar el tipo de interfaz y el número para el router Cisco IOS.
8. Router(config-if)#**ip unnumbered fastethernet 0/0.1**
9. Introduzca el comando **service-module ip address cue-ip address subnet-mask** para especificar la dirección IP de la interfaz del módulo Cisco Unity Express. La dirección IP debe estar en la misma subred que el router de Cisco IOS que aloja Cisco Unity Express.
10. Router(config-if) #**service-module ip address 172.22.1.155 255.255.255.0**
11. Introduzca el comando **service-module ip default-gateway ip address** para especificar la dirección IP del router Cisco IOS que aloja Cisco Unity Express.



12. Router (config-if) #**service-module ip default-gateway 172.22.1.154**

Nota: Estos pasos solo funcionan si **proxy-arp** está actualmente habilitado en la interfaz (FastEthernet0/0.1) a la que se hace referencia como sin numerar en la configuración del motor de servicio. Proxy-arp se habilita de forma predeterminada en las interfaces Ethernet y el estado operativo de proxy-arp en la interfaz se puede verificar si se ejecuta **Show ip interface FastEthernet0/0.1**. Si proxy-arp está inhabilitado, se puede volver a habilitar si emite **ip proxy-arp** en la configuración de la interfaz.

13. Introduzca el comando **exit** para finalizar la configuración de la interfaz.
14. Router (config-if) #**exit**
15. Introduzca el comando **ip route ip-address mask service-engine slot/number** para establecer una ruta estática al módulo Cisco Unity Express.
16. Router (config) #**ip route 172.22.1.155 255.255.255.255 service-engine 1/0**
17. Introduzca el comando **exit** para finalizar la configuración.
18. Router (config) #**end**

Nota: Aunque haya un modo de habilitación en la CLI del módulo de Cisco Unity Express, Cisco Unity Express no tiene funcionalidad de contraseña. Cualquier administrador de redes con acceso para habilitar el modo en el router puede acceder a la CLI de Cisco Unity Express. No hay control de contraseñas ni de ID de usuario en la CLI de Cisco Unity Express. El acceso se controla mediante el router. Si se requiere iniciar sesión, debe configurar el router con monitoreo de AAA/RADIUS del acceso de inicio de sesión.

• Configurar pares de marcado para que los teléfonos Cisco CallManager Express llamen al correo de voz de Cisco Unity Express

Se requiere un par de marcado exclusivo para facilitar la comunicación entre Cisco CallManager Express y Cisco Unity Express. El patrón de destino en el par de marcado asigna un conjunto de números de teléfono exclusivos a las aplicaciones, como Cisco Unity Express. Una cosa que debe tener en cuenta es que el número de correo de voz debe estar en el rango del patrón de destino del par de marcado y que el ephone-dn debe estar configurado para el reenvío de llamadas al número de correo de voz que activa el uso del par de marcado. El par de marcado de Cisco Unity Express debe utilizar el protocolo SIP (protocolo de inicio de sesión) para las sesiones de llamada y la traducción de los tonos de multifrecuencia bitonal (DTMF) en los mensajes de notificación del SIP. Se debe desactivar la detección de actividad de voz (VAD) y designar un códec.

1. Introduzca el comando **enable** para ingresar al modo EXEC.



2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **dial-peer voice tag voip** para definir un par de marcado con un método de encapsulación de voz.
6. Router(config)#**dial-peer voice 2 voip**
7. Introduzca el comando **destination-pattern string** para especificar el prefijo o el número E.164 completo que se utilizará para el par de marcado.
8. Router(config-dial-peer)#**destination-pattern 2...**
9. Introduzca el comando **session protocol sipv2** para especificar el SIP como protocolo de sesión para las llamadas entre el router Cisco CallManager Express del host y el módulo Cisco Unity Express.
10. Router(config-dial-peer)#**session protocol sipv2**
11. Introduzca el comando **session target ipv4:destination-ip address** para designar una dirección específica de la red para recibir llamadas de un par de marcado de voz sobre IP.
12. Router(config-dial-peer)#**session target ipv4:172.22.1.155**
13. Introduzca el comando **dtmf-relay sip-notify** para reenviar tonos DTMF mediante mensajes de notificación SIP.
14. Router(config-dial-peer)#**dtmf-relay sip-notify**
15. Introduzca el comando **codec codec** para especificar la velocidad de voz del códec de voz para un par de marcado.
16. Router(config-dial-peer)#**codec g711ulaw**

Nota: Asegúrese siempre de que no haya ninguna discrepancia entre los códecs, dado que puede dar lugar a una falla de llamada entrante o saliente.

17. Introduzca el comando **no vad** para inhabilitar VAD para las llamadas que utilizan un par de marcado determinado.
18. Router(config-dial-peer)#**no vad**
19. Introduzca el comando **exit** para finalizar la configuración.
20. Router(config-dial-peer)#**end**

• Configurar el acceso al correo de voz

La configuración de Cisco CallManager Express debe incluir la creación de un número de correo de voz que esté dentro del rango del patrón de destinos para el par de marcado creado previamente. El número del correo de voz es el número de teléfono que se marca cuando se presiona el botón de mensajes en un teléfono IP de Cisco o se reenvía una llamada ocupada o sin respuesta al correo de voz. Complete estos pasos para configurar su número de teléfono de correo de voz. También se deben configurar los ephone-dn para reenviar las llamadas ocupadas o sin respuesta al número de correo de voz.



1. Introduzca el comando **enable** para ingresar al modo EXEC.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **telephony-service** para ingresar al modo de configuración del servicio de telefonía.
6. Router(config)#**telephony-service**
7. Ingrese el comando voicemail **phone-number** para definir el número marcado cuando se presiona el botón Mensajes.
8. Router(config-telephony-service)#**voicemail 2000**
9. Introduzca el comando **exit** para finalizar la configuración.
10. Router(config-telephony-service)#**exit**
11. Introduzca el comando **ephone-dn dn-tag** para ingresar al modo de configuración ephone-dn para modificar las extensiones creadas previamente.
12. Router(config)#**ephone-dn 11**
13. Introduzca el comando **call-forward busy directory-number** para configurar el desvío de llamadas de modo que las llamadas entrantes a una extensión ocupada se reenvíen al buzón de voz.
14. Router(config-ephone-dn)#**call-forward busy 2000**
15. Introduzca el comando **call-forward noan directory number timeout seconds** para configurar el desvío de llamadas de modo que las llamadas entrantes a una extensión sin respuesta se reenvíen al buzón de voz.
16. Router(config-ephone-dn)#**call-forward noan 2000 time 10**
17. Introduzca el comando **end** para finalizar la configuración.
18. Router(config-ephone-dn)#**end**

Nota: Repita los pasos 6 a 9 en todos los teléfonos IP de Cisco conectados al sistema.

• Configurar los MWI

El mecanismo del indicador de mensajes en espera (MWI) enciende el indicador luminoso en los teléfonos IP de Cisco para informar al usuario que hay un mensaje de correo de voz en espera. El MWI se inicia después de que una persona deja un mensaje de correo de voz y se apaga después de que el usuario lo escucha. Cree dos ephone-dn, uno con la función MWI encendida (por ejemplo, ephone-dn 8000) y el otro con la función MWI apagada (por ejemplo, ephone-dn 8001) para que el mecanismo MWI funcione.

Cuando una extensión recibe una llamada (ext. 1001) y no se responde, el teléfono IP reenvía la llamada al buzón de voz donde la persona deja un mensaje. Una vez que se registra el mensaje, Cisco Unity Express realiza una llamada de notificación MWI al ephone-dn de procesamiento MWI (ext. 8000) y anexa la extensión (ext. 1001) como ID de



la parte que llama para la llamada de notificación. El número marcado es 80001001. La luz enciende la extensión (ext. 1001).

Cuando el usuario de la extensión (ext. 1001) escucha todo el correo de voz, Cisco Unity Express realiza una llamada de notificación MWI al ephone-dn de procesamiento MWI (ext. 8001) y anexa la extensión (ext. 1001) como ID de la parte que llama para la llamada de notificación. Se marca el número 80011001. Después de que el usuario escucha el correo de voz, la luz se apaga. Este es el procedimiento para configurar los ephone-dn para el MWI:

1. Introduzca el comando **enable** para ingresar al modo EXEC.
2. Router>**enable**
3. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
4. Router#**configure terminal**
5. Introduzca el comando **ephone-dn** para crear las extensiones para las líneas de teléfono IP de Cisco.
6. Router (config) #**ephone-dn 14**
7. Introduzca el comando **number number** para asociar un teléfono o una extensión con el ephone-dn.
8. Router (config-ephone-dn) #**number 8000....**
9. Introduzca el comando **mwI [on|off]** para configurar ephone-dns específicos para recibir la notificación MWI de un sistema de correo de voz externo.
10. Router (config-ephone-dn) #**mwI on**
11. Introduzca el comando **end** para finalizar la configuración.
12. Router (config-ephone-dn) #**end**

Nota: Repita el mismo procedimiento para crear una extensión 8001 con el MWI apagado.

• Configurar la aplicación de correo de voz

De ahora en adelante, la mayor parte de las configuraciones debe realizarse en el módulo NM-Cisco Unity Express real; esto significa que la conexión debe establecerse del router al módulo. Cisco Unity Express tiene modos de configuración y EXEC, que actúan similarmente a los modos de configuración y EXEC para los comandos CLI de Cisco IOS. Ejecute el comando **service-module service-engine 1/0 session** para ingresar a Cisco Unity Express. Este es el procedimiento para configurar el correo de voz:

1. Introduzca el comando **service-module service-engine 1/0 session** para conectarse al módulo.
2. Router#**service-module service-engine 1/0 session**
3. Introduzca el comando **enable** para ingresar al modo EXEC.
4. se-172-22-1-155>**enable**
5. Introduzca el comando **configure terminal** para ingresar al modo de configuración.



6. `se-172-22-1-155#configure terminal`
7. Introduzca el comando **ccn application voicemail** para ingresar la configuración de la aplicación para el buzón de voz.
8. `se-172-22-1-155 (config) #ccn application voicemail`
9. Introduzca el comando **description "text"** para introducir una descripción de la aplicación.
10. `se-172-22-1-155 (config-application) #description "Cisco Voicemail"`
11. Introduzca el comando **maxsessions number** para especificar el número de suscriptores que pueden acceder a esta aplicación simultáneamente.
12. `se-172-22-1-155 (config-application) #maxsessions 4`
13. Introduzca el comando **exit** para finalizar la configuración de la aplicación.
14. `se-172-22-1-155 (config-application) #exit`
15. Introduzca el comando **exit** para finalizar el modo de configuración.
16. `se-172-22-1-155 (config) #exit`

- **Configurar la aplicación de contestador automático**

La aplicación del contestador automático permite que el sistema tenga un operador automático que responda las llamadas y ofrezca a la persona que llama diversas opciones para elegir de un menú. Por ejemplo, si los sistemas Cisco Unity Express tienen un contestador automático, la persona que llama escuchará un saludo de bienvenida y podrá elegir una opción de transferencia a un departamento específico (por ejemplo, Ventas, Recursos Humanos, etc.) o a una persona específica (por ejemplo, John Smith, Alex Lewis, etc.). Este procedimiento proporciona la configuración para el contestador automático:

1. Introduzca el comando **service-module service-engine slot/number session** para conectarse al módulo.
2. `Router#service-module service-engine 1/0 session`
3. Introduzca el comando **enable** para ingresar al modo EXEC.
4. `se-172-22-1-155#enable`
5. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
6. `se-172-22-1-155#configure terminal`
7. Introduzca el comando **ccn application autoattendant** para especificar la aplicación a configurar.
8. `se-172-22-1-155 (config) #ccn applicatio autoattendant`
9. Introduzca el comando **description "text"** para introducir una descripción de la aplicación.
10. `se-172-22-1-155 (config-application) #description "Cisco Auto-Attendant"`



11. Introduzca el comando **maxsessions number** para especificar el número de personas que llaman que pueden acceder a esta aplicación simultáneamente.
12. `se-172-22-1-155 (config-application) #maxsessions 4`
13. Introduzca el comando **parameter "name" "value"** para especificar el parámetro para la aplicación.
14. `se-172-22-1-155 (config-application) #parameter "operExtn" "1001"`
15. Introduzca el comando **exit** para finalizar la configuración de la aplicación.
16. `se-172-22-1-155 (config-application) #exit`
17. Introduzca el comando **exit** para finalizar la configuración.
18. `se-172-22-1-155 (config) #exit`

• Configurar los activadores SIP para las aplicaciones

Una vez configurados el correo de voz y el contestador automático, debe configurarse el sistema para iniciar las aplicaciones del contestador automático y el correo de voz cuando se invoca una señal o un activador específicos. El activador es un número de teléfono. Cuando la persona que llama marca un número de teléfono especificado, el subsistema del SIP inicia el correo de voz o el contestador automático. Este procedimiento configura los activadores del SIP para el correo de voz:

1. Introduzca el comando **service-module service-engine slot/number session** para conectarse al módulo.
2. Router#**service-module service-engine 1/0 session**
3. Introduzca el comando **enable** para ingresar al modo EXEC.
4. `se-172-22-1-155>enable`
5. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
6. `se-172-22-1-155#configure terminal`
7. Introduzca el comando **ccn trigger sip phonenumber number** para especificar el número de teléfono que actúa como modo de configuración del disparador. El valor numérico puede coincidir con uno de los patrones configurados en el campo de patrón de destino del par de marcado del SIP que apunta a Cisco Unity Express.
8. `se-172-22-1-155 (config) #ccn trigger sip phonenumber 2000`
9. Introduzca el comando **application string** para especificar el nombre de la aplicación que se iniciará cuando se introduzca el disparador.
10. `se-172-22-1-155 (config-trigger) #application voicemail`
11. Introduzca el comando **enabled** para habilitar el disparador.
12. `se-172-22-1-155 (config-trigger) #enabled`
13. Introduzca el comando **maxsessions number** para especificar el número máximo de personas que llaman que la aplicación puede manejar simultáneamente.
14. `se-172-22-1-155 (config-trigger) #maxsessions 4`
15. Introduzca el comando **exit** para finalizar la configuración del disparador.



16. `se-172-22-1-155 (config-trigger) #exit`
17. Introduzca el comando **exit** para finalizar la configuración.
18. `se-172-22-1-155 (config) #exit`

Nota: Repita este proceso para el contestador automático y la aplicación `promptmgmt`.

• Configurar usuarios

Pueden crearse usuarios y grupos para que utilicen el sistema. Todas las personas con extensiones y acceso al correo de voz deben ser usuarios. Se crea un usuario administrador de forma predeterminada cuando accede por primera vez a Cisco Unity Express. No se puede asignar un buzón de correo de voz a este administrador. Sin embargo, el administrador puede configurar el sistema, que incluye la aplicación del contestador automático y el correo de voz. Este procedimiento crea un usuario y asigna un número de teléfono:

1. Introduzca el comando **service-module service-engine slot/number session** para conectarse al módulo.
2. Router#**service-module service-engine 1/0 session**
3. Introduzca el comando **enable** para ingresar al modo EXEC.
4. `se-172-22-1-155>enable`
5. Introduzca el comando **username userid create** para crear un suscriptor con el ID de usuario especificado.
6. `se-172-22-1-155#username John create`
7. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
8. `se-172-22-1-155#configure terminal`
9. Introduzca el comando **username userid phoneumber number** para especificar la extensión para este suscriptor.
10. `se-172-22-1-155 (config) #username John phonenumber 1002`
11. Introduzca el comando **exit** para finalizar la configuración.
12. `se-172-22-1-155 (config) #exit`

Nota: Repita este proceso para registrar tantos usuarios como necesite, sin exceder el límite admitido por el sistema de Cisco Unity Express. Asegúrese de asignar una contraseña y un PIN al usuario administrador para que pueda configurar Cisco Unity Express y realizar cambios.

• Configurar buzones

Asigne un buzón de correo de voz a un suscriptor para configurar una base de datos de Cisco Unity Express. Un suscriptor del buzón es un usuario creado en la sección anterior. No todos los suscriptores o las extensiones requieren un buzón de correo de voz, como un



usuario administrador. Tenga en cuenta la función o el propósito del suscriptor o la extensión antes de asignar un buzón para utilizar los buzones eficientemente.

Los correos de voz no están comprimidos y utilizan el códec G.711. Cada segundo de audio G.711 equivale a 64 kbits (kb)/segundo; 8 k bytes (kB)/segundo se convierten en 480 kB/minuto. Esta lista muestra un resumen de la capacidad de almacenamiento para cada tipo de módulo de Cisco Unity Express:

- Cisco Unity Express Advanced Integration Module (AIM-CUE): 14 horas
- Cisco Unity Express Network Module (NM-CUE): 100 horas
- Cisco Unity Express Enhanced Capacity (NM-CUE-EC): 300 horas

En esta configuración, se crea un buzón personal. Un buzón personal se asigna a un suscriptor específico y solo este suscriptor puede acceder a él. Cuando la persona que llama deja un mensaje en este buzón, se enciende la luz del MWI. Complete estos pasos para configurar los buzones de correo de voz:

1. Introduzca el comando **service-module service-engine slot/number session** para conectarse al módulo.
2. Router#**service-module service-engine 1/0 session**
3. Introduzca el comando **enable** para ingresar al modo EXEC.
4. se-172-22-1-155>**enable**
5. Introduzca el comando **configure terminal** para ingresar al modo de configuración.
6. se-172-22-1-155#**configure terminal**
7. Introduzca el comando **voice mailbox owner name** para crear un buzón para el valor de nombre.
8. se-172-22-1-155 (config) #**voice mailbox owner John**
9. Introduzca el comando **description "text"** para proporcionar una descripción del buzón.
10. se-172-22-1-155 (config-mailbox) #**description "John's Mailbox"**
11. Introduzca el comando **enable** para activar el nuevo buzón o reactivar el buzón deshabilitado.
12. se-172-22-1-155 (config-mailbox) #**enable**
13. Introduzca el comando **expiration time days** para establecer el número de días para los que se almacenan los mensajes en el buzón. El valor predeterminado es 30 días.
14. se-172-22-1-155 (config-mailbox) #**expiration time 10**
15. Introduzca el comando **mailboxsize seconds** para especificar el tamaño de almacenamiento del buzón en segundos.
16. se-172-22-1-155 (config-mailbox) #**mailboxsize 300**
17. Introduzca el comando **messagesize seconds** para especificar el tamaño máximo de un mensaje entrante, en segundos.
18. se-172-22-1-155 (config-mailbox) #**messagesize 120**



19. Introduzca el comando **end** para finalizar la configuración del buzón.

20. `se-172-22-1-155 (config-mailbox) #end`

21. Introduzca el comando **exit** para finalizar la configuración.

22. `se-172-22-1-155 (config) #exit`

Nota: Repita este procedimiento para cada usuario que necesite un buzón de correo de voz.

Anexo IV:

Cisco 4351

Se muestra el router elegido con sus especificaciones y características.



Ilustración 16. CME Cisco 4351. Fuente: Cisco

Network interface modules (NIM)

3

Maximum switched Ethernet LAN ports with PoE

48

EtherSwitch Service Module type (width)

2 single or 1 double

PoE support (wattage) without PoE boost

500 W

Intrusion prevention

Yes

**Cisco Cloud Web Security**

Yes

Form factor

2 RU

SSL VPN

No

Module online insertion and removal (OIR)

es

Power supply type

Internal; AC, PoE or DC

Maximum switched Ethernet ports

48

Hardware VPN acceleration (DES, 3DES, AES)

No

Redundant power supply

No

Management port

1 GE (Integrated Out of Band)

PoE support (wattage) with PoE boost

990 W

Integrated Services Card (ISC) slots

1 (PVDM 4)

Server virtualization platform (UCS E-Series)

2 core single-wide, 4 core single-wide, 4 core double-wide, 6 core double-wide, 8 core double-wide

Enhanced Services Module (SM-X)

2 single or 1 double-wide

Identity-based networking

No

Zone-based firewall and NAT services

VRF-Aware Firewall and Network Address Translation (NAT)

USB Ports (type A)

2

Integrated WAN ports

2 PoE GE / SFP; 1 GE / SFP

**Default/max DRAM**

4 GB / 16 GB

Default/max Flash

4 GB / 16 GB

Performance

200 Mbps upgradeable to 400 Mbps

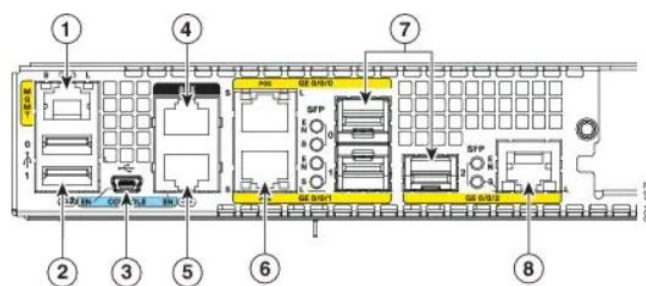
Figure 1-17 Power Supply and Bezel Side View of Cisco 4351 ISR



1	Power supply unit	2	Router fan tray (hidden behind the removable bezel)
3	LEDs	4	Router power On/Off switch

Ilustración 17. Frontal CME Cisco 4351. Fuente: Cisco

Figure 1-19 Ports on Cisco 4351 ISR



1	GE management port	2	USB Type A port
3	USB Type B mini port	4	Auxiliary port
5	Console port	6	RJ-45 port (GE 0/0/0, GE 0/0/1)
7	SFP port (GE 0/0/0, GE 0/0/1, GE 0/0/2)	8	RJ-45 port (GE/0/0/2)

Ilustración 18. Parte posterior del CME Cisco 4351. Fuente: Cisco



Anexo V:

Modelo cuestionario sobre CM

Esta encuesta tiene el objeto de obtener información sobre las centralitas IP, para realizar el trabajo de fin de grado: “Desarrollo de las comunicaciones VoIP a través de un Call Manager”.

La población objetivo de este cuestionario será personal de la BRIPAC suboficial u oficial que haya trabajado y manipulado el sistema desde su llegada a la unidad hasta ahora en 2022.

1. **¿Para qué se usa el CM en la unidad?**
2. **¿Qué opciones de desarrollo tiene el CM que aún no se está explotando?**
3. **¿Qué uso puede tener el CM en operaciones?**
4. **¿Qué relación hay entre la operatividad y la seguridad con un CM?**
5. **¿Qué CM recomendaría adquirir a la unidad?**
6. **¿Qué problemas tiene el CM a la hora de integrarlo en la red? ¿Qué aspectos limitan o impiden más su operación?**

Anexo VI:

En este anexo se detalla el proceso de las solicitudes o peticiones SIP, que se clasifican en categorías, denominadas métodos. Cada método tiene una función determinada en la arquitectura SIP. La RFC (Request for Comments) 3261 define 6 métodos.

- INVITE: se utiliza para establecer sesiones y anunciar capacidades del nodo SIP.
- ACK: confirma que el cliente solicitante ha recibido una respuesta final desde un servidor a una solicitud INVITE.
- OPTIONS: se utiliza para preguntar a un nodo SIP sus capacidades, antes de establecer un canal multimedia.
- BYE: una vez establecida la llamada, se utiliza para anunciar que un extremo ha decidido finalizar la llamada.
- CANCEL: sirve para cancelar una solicitud pendiente antes de que se complete.
- REGISTER: se utiliza para solicitar el registro del usuario en un servidor SIP de registro.

Existen nuevas extensiones SIP que definen nuevos métodos.



- INFO: permite enviar señales de aplicación por el canal de señalización.
- PRACK: es utilizado en lugar del ACK para notificar al otro extremo que hay una llamada establecida.
- SUBSCRIBE: proporciona una manera de establecer reguladores de eventos en la aplicación SIP.
- NOTIFY: se usa para entregar eventos ocurridos durante la llamada entre extremos SIP.

Por otro lado, se encuentran las respuestas. Cuando se produce algún evento, se envía un mensaje; cada mensaje tiene una respuesta de 3 dígitos y una descripción, clasificándose así:

- 1xx. Aún no ha terminado la transacción. es de carácter informativo.
- 2xx. Éxito. La solicitud ha sido atendida de manera exitosa.
- 3xx. Respuesta de redireccionamiento. Se complementa con información acerca de donde enviar la siguiente petición.
- 4xx. Error del cliente. Sintaxis errónea.
- 5xx error del servidor. El servidor no ha podido resolver la solicitud.
- 6xx. Fallo global. Ningún servidor puede resolver la solicitud.

Estas respuestas siguen una estructura similar a HTTP. [\[9\]](#)

Anexo VII:

En este anexo se muestra el extracto de BOE donde se aprecia la nueva estructuración de la BRIPAC dentro de la División “San Marcial”.

BOE Núm. 204 martes 28 de julio de 2020 Sec. I. Pág. 58821



Artículo 13. *La División «San Marcial».*

1. La División «San Marcial» es un conjunto de unidades especializadas puestas bajo un mando único, organizadas, equipadas y preparadas para constituir organizaciones operativas capaces de integrarse en estructuras fundamentalmente conjuntas y combinadas, y que tienen por cometido principal la preparación de sus unidades, así como la generación de las fuerzas que se le requieran.

2. La División «San Marcial» se articula en:

- a) El Cuartel General de la División San Marcial.
- b) La Brigada «Almogávares» VI de Paracaidistas.
- c) El Mando de Tropas de Montaña.
- d) El Mando de Operaciones Especiales «Órdenes Militares».
- e) Las Fuerzas Aeromóviles del Ejército de Tierra.
- f) Las pequeñas Unidades que se determinen.

3. El Cuartel General de la División San Marcial asistirá al Jefe de la División en el ejercicio del mando y en la preparación de sus unidades.

4. La Brigada «Almogávares» VI de Paracaidistas, como Brigada del Ejército de Tierra, está organizada para actuar como tal en operaciones militares que requieran una respuesta inicial ante una crisis. Proporciona la capacidad paracaidista del Ejército de Tierra. Además, junto con otras unidades, proporciona Fuerzas de Apoyo a unidades de Operaciones Especiales, en aquellas operaciones que lo exijan.

5. El Mando de Tropas de Montaña es un conjunto de unidades puestas bajo un mando único, organizadas, equipadas y adiestradas para proporcionar la capacidad de vida, movimiento y combate en zonas de montaña y de clima frío extremo, a aquellas operaciones que exijan disponer de dichas capacidades.

6. El Mando de Operaciones Especiales «Órdenes Militares» es un conjunto de unidades de operaciones especiales y de unidades de apoyo, puestas bajo un mando único, organizadas, equipadas y adiestradas para realizar operaciones especiales en aquellas operaciones que exijan disponer de dicha capacidad.

7. Las Fuerzas Aeromóviles del Ejército de Tierra son un conjunto de unidades de combate, de apoyo al combate y de apoyo logístico al combate, dotadas de aeronaves, puestas bajo un mando único, organizadas, equipadas y adiestradas para proporcionar la capacidad de la maniobra aeromóvil constituyendo organizaciones operativas que operan en el ámbito aeroterrestre, siendo empleadas en apoyo de las unidades que se determinen o en el marco de otras organizaciones.

Figura 27. Extracto de organización. Fuente: Defensa